

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-351324

(P2001-351324A)

(43) 公開日 平成13年12月21日 (2001. 12. 21)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト*(参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 C 0 5 3
20/12		20/12	5 D 0 4 4
H 0 4 L 9/16		H 0 4 L 9/00	6 4 3 5 J 1 0 4
H 0 4 N 5/91		H 0 4 N 5/91	P
5/92		5/92	H
審査請求 未請求 請求項の数47 O L (全 52 頁)			

(21) 出願番号 特願2000-243207 (P2000-243207)

(22) 出願日 平成12年8月10日 (2000. 8. 10)

(31) 優先権主張番号 特願2000-101862 (P2000-101862)

(32) 優先日 平成12年4月4日 (2000. 4. 4)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(72) 発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

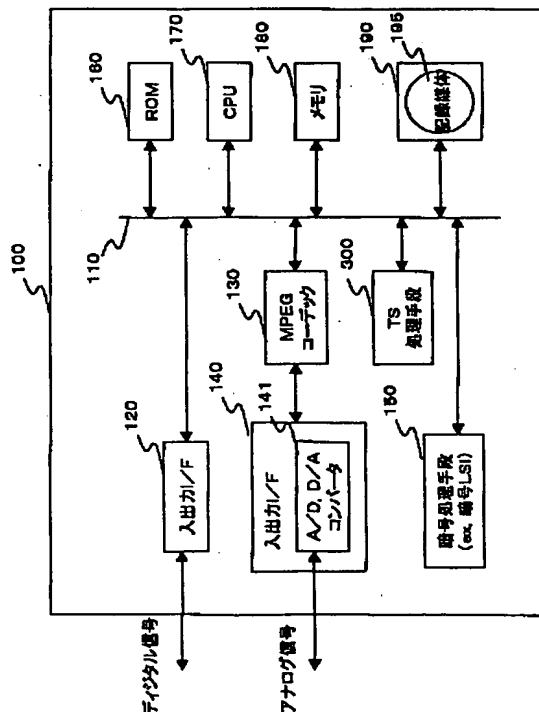
最終頁に続く

(54) 【発明の名称】 情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体

(57) 【要約】

【課題】 ブロックごとに異なる暗号鍵を用いた暗号化構成を記録媒体上に鍵格納領域を形成せずに可能とする情報記録再生装置を提供する。

【解決手段】 トランスポートストリームを構成するランスポートパケットの着信時刻に応じて付加されるATSを用いてブロック・データを暗号化するブロックキーを生成する。ATSは時刻に応じたランダムなデータであるので、ブロック毎に異なる固有キーを生成でき、暗号解析に対する強度が高まる。ブロックキーは、ATSと、マスターキー、ディスク固有キー、タイトル固有キー等、デバイス、記録媒体に固有の鍵を組み合わせで生成する。ATSを用いてブロックキーを生成することにより、ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となる。



【特許請求の範囲】

【請求項1】記録媒体に情報を記録する情報記録装置において、

間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ATS）を付加するトランスポート・ストリーム処理手段と、

前記受信時刻情報（ATS）の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理手段と、を有し、

前記暗号処理手段によって暗号化したデータを前記記録媒体に記録する構成としたことを特徴とする情報記録装置。

【請求項2】前記暗号処理手段は、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする請求項1に記載の情報記録装置。

【請求項3】前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする請求項1に記載の情報記録装置。

【請求項4】前記暗号処理手段は、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項5】前記ブロックシードは、前記受信時刻情報（ATS）の他にコピー制御情報を含むデータであることを特徴とする請求項1に記載の情報記録装置。

【請求項6】前記暗号処理手段は、前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化する構成であることを特徴とする請求項1に記載の情報記録装置。

【請求項7】前記暗号処理手段は、

情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求項1に記載の情報記録装置。

【請求項8】前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求項1に記載の情報記録装置。

【請求項9】前記暗号処理手段は、該暗号処理手段を構成するLSIに格納されたLSIキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、またはこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする請求項1に記載の情報記録装置。

【請求項10】前記暗号処理手段は、前記ブロックデータに対するブロックキーによる暗号処理をDESアルゴリズムに従って実行する構成であることを特徴とする請求項1に記載の情報記録装置。

【請求項11】前記情報記録装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項12】前記情報記録装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする請求項1に記載の情報記録装置。

【請求項13】記録媒体から情報を再生する情報再生装置において、前記記録媒体に記録された暗号データを復号する暗号処理手段であり、

複数のトランスポートパケットの各々に受信時刻情報（ATS）を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する暗号処理手段と、
前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報（ATS）に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段と、を有することを特徴とする情報再生装置。

【請求項14】前記暗号処理手段は、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする請求項13に記載の情報再生装置。

【請求項15】前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする請求項13に記載の情報再生装置。

【請求項16】前記ブロックシードは、前記受信時刻情報（ATS）の他にコピー制御情報を含むデータであることを特徴とする請求項13に記載の情報再生装置。

【請求項17】前記暗号処理手段は、前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより復号する構成であることを特徴とする請求項13に記載の情報再生装置。

【請求項18】前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求項13に記載の情報再生装置。

【請求項19】前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒

体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする請求項13に記載の情報再生装置。

【請求項20】前記暗号処理手段は、該暗号処理手段を構成するLSIに格納されたLSIキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、またはこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする請求項13に記載の情報再生装置。

【請求項21】前記暗号処理手段は、前記ブロックデータに対するブロックキーによる復号処理をDESアルゴリズムに従って実行する構成であることを特徴とする請求項13に記載の情報再生装置。

【請求項22】前記情報再生装置は、記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて再生実行の可否を制御する構成を有することを特徴とする請求項13に記載の情報再生装置。

【請求項23】前記情報再生装置は、記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、

前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator) を識別し、該EMIに基づいて再生実行の可否を制御する構成を有することを特徴とする請求項13に記載の情報再生装置。

【請求項24】記録媒体に情報を記録する情報記録方法において、

トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ATS）を付加するトランスポート・ストリーム処理ステップと、前記受信時刻情報（ATS）の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有し、

前記暗号処理ステップによって暗号化したデータを前記記録媒体に記録することを特徴とする情報記録方法。

【請求項25】前記暗号処理ステップは、

前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 2 6】前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスク ID と、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 2 7】前記情報記録方法は、さらに、記録媒体固有の記録媒体識別子であるディスク ID と、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する識別子生成ステップを有することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 2 8】前記暗号処理ステップは、前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 2 9】前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスク ID と、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 3 0】前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスク ID と、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 3 1】前記暗号処理ステップは、暗号処理手段を構成する LSI に格納された LSI キー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、またはこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用の

ブロックキーを生成することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 3 2】前記暗号処理ステップは、前記ブロックデータに対するブロックキーによる暗号処理を DES アルゴリズムに従って実行することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 3 3】前記情報記録方法は、さらに、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 3 4】前記情報記録方法は、さらに、コピーを制御するためのコピー制御情報としての 2 ビットの EMI (Encryption Mode Indicator) を識別し、該 EMI に基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする請求項 2 4 に記載の情報記録方法。

【請求項 3 5】記録媒体から情報を再生する情報再生方法において、

複数のトランスポートパケットの各々に受信時刻情報 (ATS) を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報 (ATS) に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、を有することを特徴とする情報再生方法。

【請求項 3 6】前記復号処理ステップは、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする請求項 3 5 に記載の情報再生方法。

【請求項 3 7】前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスク ID と、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする請求項 3 5 に記載の情報再生方法。

【請求項 3 8】前記復号処理ステップは、前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより復

号することを特徴とする請求項35に記載の情報再生方法。

【請求項39】前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求項35に記載の情報再生方法。

【請求項40】前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする請求項35に記載の情報再生方法。

【請求項41】前記復号処理ステップは、暗号処理手段を構成するLSIに格納されたLSIキー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、またはこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする請求項35に記載の情報再生方法。

【請求項42】前記復号処理ステップは、前記ブロックデータに対するブロックキーによる復号処理をDESアルゴリズムに従って実行することを特徴とする請求項35に記載の情報再生方法。

【請求項43】前記情報再生方法は、さらに、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする請求項35に記載の情報再生方法。

【請求項44】前記情報再生方法は、さらに、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする請求項35に記載の情報再生方法。

【請求項45】トランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加した1以上のパケットからなるブロックデータの暗号化鍵として使用されるブロックキーの生成情報となる受信時刻情報(ATS)を含むブロックシードを有する非暗号化データ部

と、前記ブロックキーにより暗号化された暗号化データ部と、を構成要素とするブロックデータを記録したことを特徴とする記録媒体。

【請求項46】記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理ステップと、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体。

【請求項47】記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数のトランスポートパケットの各々に受信時刻情報(ATS)を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、データ記録再生可能な記録媒体に対するデータ書き込み、データ再生処理における違法コピーを防止することを可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関する。

【0002】

【従来の技術】ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録す

る記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【0003】例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインターフェース（DIF）から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【0004】具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、1度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー（copy free）となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可（copy once allowed）となっている場合には、SCMS信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【0005】しかしながら、SCMSは上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピー

を防止する構成となっている。

【0006】コンテンツ・スクランブルシステムでは、DVD-ROM（Read Only Memory）に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

【0007】一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

【0008】しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ROMメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、RAMメディアという）への適用については考慮されていない。

【0009】即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【0010】そこで、本出願人は、先の特許出願、特開平11-224461号公報（特願平10-25310号）において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【0011】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【0012】ライセンスを受けていない装置は、媒体識

別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【0013】

【発明が解決しようとする課題】ところで、特開平11-224461号公報（特願平10-25310号）において開示している構成は、ディスクに記録する画像、音声、プログラム等のコンテンツデータを各セクタごとに個別の鍵セクタキーを用いて暗号化する構成としている。

【0014】これは、1つの暗号鍵で大量のデータを暗号化すると、媒体上に格納された暗号文と、なんらかの手段で攻撃者が入手した平文の組を用いて、差分攻撃や線形攻撃などの暗号攻撃の手法により、暗号鍵が露呈しやすくなるという課題に対処するためである。上記の出願ではセクタという決まった大きさごとに暗号鍵を変えることにより、1つの暗号鍵で処理するデータの量を小さく押さえて暗号鍵の解読を困難にすることができる。さらに、万が一鍵が解読された場合においても復号可能なデータ量を少なくすることができる。

【0015】しかしながら、上記公報に記載の例では、コンテンツの暗号化に使用したセクタ毎の暗号鍵（セクタキー）をさらに上位の鍵で暗号化して、記録媒体のセクタヘッダに格納している。このため、セクタヘッダに暗号化したセクタキーを格納するだけの領域が必要になり、また、コンテンツの記録、再生時に、メインデータ部だけでなく、セクタヘッダにアクセスをして暗号化セクタキーの書きこみ（記録時）もしくは読出し（再生時）を行わなければならない。

【0016】本発明は、上述のような従来技術の問題点を解決することを目的とするものであり、ブロックデータの暗号化処理を異なる鍵で実行可能として暗号解析に対する強度を高めることができる構成とするとともに、暗号鍵の格納領域をディスク上に新たに設ける必要を排除してデータ領域を狭めることのない構成を実現する情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供する。

【0017】より、具体的には、本発明は、データを構成するトランスポートストリームに含まれる各パケットの着信時刻に応じたランダム性のあるデータとして構成されるATSを用いてブロックデータを暗号化するブロックキーを生成する構成としてブロック毎に異なる固有キーを生成することで、暗号解析に対する強度を高

め、また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域を不要としてメインデータ領域を有効に使用可能とする情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

【0018】

【課題を解決するための手段】本発明の第1の側面は、記録媒体に情報を記録する情報記録装置において、間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報（ATS）を付加するトランスポート・ストリーム処理手段と、前記受信時刻情報（ATS）の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理手段と、を有し、前記暗号処理手段によって暗号化したデータを前記記録媒体に記録する構成としたことを特徴とする情報記録装置にある。

【0019】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報（ATS）を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする。

【0020】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする。

【0021】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する構成を有することを特徴とする。

【0022】さらに、本発明の情報記録装置の一実施態様において、前記ブロックシードは、前記受信時刻情報（ATS）の他にコピー制御情報を含むデータであることを特徴とする。

【0023】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記ブロックデータの暗号処理において、該ブロックデータのブロックシー

ドを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化する構成であることを特徴とする。

【0024】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

【0025】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

【0026】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、該暗号処理手段を構成するLSIに格納されたLSIキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、またはこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する暗号処理用のブロックキーを生成する構成であることを特徴とする。

【0027】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記ブロックデータに対するブロックキーによる暗号処理をDESアルゴリズムに従って実行する構成であることを特徴とする。

【0028】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

【0029】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、記録媒体に対する記録対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御する構成を有することを特徴とする。

【0030】さらに、本発明の第2の側面は、記録媒体から情報を再生する情報再生装置において、前記記録媒体に記録された暗号データを復号する暗号処理手段であり、複数のトランスポートパケットの各々に受信時刻情報(ATS)を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する暗号処理手段と、前記暗号処理手段において復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理手段と、を有することを特徴とする情報再生装置にある。

【0031】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする。

【0032】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成する構成であることを特徴とする。

【0033】さらに、本発明の情報再生装置の一実施態様において、前記ブロックシードは、前記受信時刻情報(ATS)の他にコピー制御情報を含むデータであることを特徴とする。

【0034】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより復号する構成であることを特徴とする。

【0035】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

【0036】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方方向関数に入力して暗号化した結果をブロックキーとして出力する構成であることを特徴とする。

【0037】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、該暗号処理手段を構成するLSIに格納されたLSIキー、前記情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、またはこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成する構成であることを特徴とする。

【0038】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記ブロックデータに対するブロックキーによる復号処理をDESアルゴリズムに従って実行する構成であることを特徴とする。

【0039】さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて再生実行の可否を制御する構成を有することを特徴とする。

【0040】さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、記録媒体からの再生対象となる情報を受信するインタフェース手段を有し、前記インタフェース手段は、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator)を識別し、該EMIに基づいて再生実行の可否を制御する構成を有することを特徴とする。

【0041】さらに、本発明の第3の側面は、記録媒体に情報を記録する情報記録方法において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理ステップと、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有し、前記暗号処理ステップによって暗号化したデータを前記記録媒体に記録することを特徴とする情報記録方法にある。

【0042】さらに、本発明の情報記録方法の一実施態

様において、前記暗号処理ステップは、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする。

【0043】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードとに基づいてブロックキーを生成することを特徴とする。

【0044】さらに、本発明の情報記録方法の一実施態様において、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとを生成して前記記録媒体に格納する処理を実行する識別子生成ステップを有することを特徴とする。

【0045】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記ブロックデータの暗号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成データのみを前記ブロックキーにより暗号化することを特徴とする。

【0046】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

【0047】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方方向関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

【0048】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、暗号処理手段を構成するLSIに格納されたLSIキー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、またはこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記

ブロックデータに対する暗号処理用のブロックキーを生成することを特徴とする。

【0049】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記ブロックデータに対するブロックキーによる暗号処理をDESアルゴリズムに従って実行することを特徴とする。

【0050】さらに、本発明の情報記録方法の一実施態様において、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする。

【0051】さらに、本発明の情報記録方法の一実施態様において、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator) を識別し、該EMIに基づいて記録媒体に対する記録実行の可否を制御するコピー制御ステップを有することを特徴とする。

【0052】さらに、本発明の第4の側面は、記録媒体から情報を再生する情報再生方法において、複数のトランスポートパケットの各々に受信時刻情報(ATS)を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、を有することを特徴とする情報再生方法にある。

【0053】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記ブロックデータを構成する複数のトランスポートパケットの先頭のトランスポートパケットに付加された受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて、前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする。

【0054】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、該タイトル固有キーと前記ブロックシードに基づいてブロックキーを生成することを特徴とする。

【0055】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記ブロックデータの復号処理において、該ブロックデータのブロックシードを含む先頭領域データ以外のブロックデータ構成

データのみを前記ブロックキーにより復号することを特徴とする。

【0056】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーを暗号関数の鍵とし、前記ブロックシードを前記暗号関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

【0057】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、情報記録装置に格納されたマスターキーと、記録媒体固有の記録媒体識別子であるディスクIDと、前記記録媒体に記録すべきデータ固有のタイトルキーとに基づいてタイトル固有キーを生成し、生成したタイトル固有キーと、前記ブロックシードとを一方関数に入力して暗号化した結果をブロックキーとして出力することを特徴とする。

【0058】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、暗号処理手段を構成するLSIに格納されたLSIキー、情報記録装置に格納されたデバイスキー、前記記録媒体に格納されたメディアキー、前記記録媒体のドライブ装置に格納されたドライブキーのいずれか、またはこれら各キーの組合わせに基づいてデバイス固有キーを生成し、生成したデバイス固有キーと前記ブロックシードとに基づいて前記ブロックデータに対する復号処理用のブロックキーを生成することを特徴とする。

【0059】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記ブロックデータに対するブロックキーによる復号処理をDESアルゴリズムに従って実行することを特徴とする。

【0060】さらに、本発明の情報再生方法の一実施態様において、前記トランスポートストリームを構成する各パケットに付加されたコピー制御情報を識別し、該コピー制御情報に基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする。

【0061】さらに、本発明の情報再生方法の一実施態様において、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator) を識別し、該EMIに基づいて記録媒体からの情報再生実行の可否を制御するコピー制御ステップを有することを特徴とする。

【0062】さらに、本発明の第5の側面は、トランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加した1以上のパケットからなるブロックデータの暗号化鍵として使用されるブロックキーの生成情報となる受信時刻情報(ATS)を含むブロックシ

ードを有する非暗号化データ部と、前記ブロックキーにより暗号化された暗号化データ部と、を構成要素とするブロックデータを記録したことを特徴とする記録媒体にある。

【0063】さらに、本発明の第6の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、間欠的なトランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報(ATS)を付加するトランスポート・ストリーム処理ステップと、前記受信時刻情報(ATS)の付加された1以上のパケットからなるブロックデータに対する暗号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【0064】さらに、本発明の第7の側面は、記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、複数のトランスポートパケットの各々に受信時刻情報(ATS)を付加したブロックデータの暗号化データに対する復号処理用のブロックキーを前記受信時刻情報(ATS)を含むブロックデータ固有の付加情報であるブロックシードに基づいて生成するとともに、生成したブロックキーによるブロックデータ毎の復号処理を実行する復号処理ステップと、前記暗号処理ステップにおいて復号されたブロックデータを構成する複数のトランスポートパケットの各々に付加された受信時刻情報(ATS)に基づいてデータ出力制御を実行するトランスポート・ストリーム処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【0065】

【作用】本発明においては、記録媒体に記録するコンテンツの形式をMPEG2.TSパケット(packet)とし、このパケットを記録装置が受信した時刻情報であるATSを付加して記録する。ATSは24乃至32ビットのデータであり、ある程度のランダム性がある。ここで、ATSはArrival Time Stamp(着信時刻スタンプ)の略である。

【0066】記録媒体のひとつのブロック(セクタ)には、ATSを付加したTSパケットをX個記録することにし、その第1番目のTSパケットに付加されたATSを用いてそのブロックのデータを暗号化するブロックキーを生成する。

【0067】このようにすることにより、各ブロックごとに固有の鍵を用いて暗号化することができ、また鍵を

格納する特別な領域も不要となり、記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなる。

【0068】さらに、TSパケットにATSだけでなくコピー制限情報(CCI:Copy Control Information)も付加して記録し、ATSとCCIを用いてブロックキーを生成するようにすることも可能である。

【0069】なお、本発明の第6および第7の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0070】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0071】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0072】

【発明の実施の形態】
 【システム構成】図1は、本発明を適用した記録再生装置100の一実施例形態の構成を示すブロック図である。記録再生装置100は、入出力I/F(Interface)120、MPEG(Moving Picture Experts Group)コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F(Interface)140、暗号処理手段150、ROM(Read Only Memory)160、CPU(Central Processing Unit)170、メモリ180、記録媒体195のドライブ190、さらにトランスポート・ストリーム処理手段(TS処理手段)300を有し、これらはバス110によって相互に接続されている。

【0073】入出力I/F120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F140に出力するとともに、入出力I/F140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F140は、外部から供

給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D(Analog Digital)変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A(Digital Analog)変換することで、アナログ信号として、外部に出力する。

【0074】暗号処理手段150は、例えば、1チップのLSI(Large Scale Integrated Circuit)で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0075】ROM160は、例えば、記録再生装置ごとに固有の、あるいは、複数の記録再生装置のグループごとに固有のデバイスキーを記憶している。CPU170は、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータを記憶する。ドライブ190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し(再生し)、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。なお、プログラムをROM160に、デバイスキーをメモリ180に記憶するように構成してもよい。

【0076】記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

【0077】トランスポート・ストリーム処理手段(TS処理手段)300は、後段において図6以下を用いて詳細に説明するが、例えば複数のTVプログラム(コンテンツ)が多重化されたトランスポートストリームから特定のプログラム(コンテンツ)に対応するトランスポート packets を取り出して、取り出したトランスポートストリームの出現タイミング情報を各 packet とともに記録媒体195に格納するためのデータ処理および、記録媒体195からの再生処理時の出現タイミング制御処理を行なう。

【0078】トランスポートストリームには、各トランスポート packets の出現タイミング情報としてのATS

(Arrival Time Stamp: 着信時刻スタンプ)が設定されており、このタイミングはMPEG2システムズで規定されている仮想的なデコーダであるTSTD(Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポート packets に付加されたATSによって出現タイミングを制御する。トランスポート・ストリーム処理手段(TS処理手段)300は、これらの制御を実行する。例えば、トランスポート packets を記録媒体に記録する場合には、各 packet の間隔を詰めたソース packets として記録するが、各トランスポート packets の出現タイミングを併せて記録媒体に保存することにより、再生時に各 packet の出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段(TS処理手段)300は、DVD等の記録媒体195へのデータ記録時に、各トランスポート packets の入力タイミングを表すATS(Arrival Time Stamp: 着信時刻スタンプ)を付加して記録する。

【0079】本発明の記録再生装置100は、上述のATSの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段150において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体195に格納する。さらに、暗号処理手段150は、記録媒体195に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

【0080】なお、図1に示す暗号処理手段150、TS処理手段300は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する1つのワンチップLSIとして構成してもよく、また、両機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。

【0081】本発明の記録再生装置の構成例としては図1に示す構成の他に図2に示す構成が可能である。図2に示す記録再生装置200では、記録媒体205はドライブ装置としての記録媒体インタフェース(I/F)210から着脱が可能であり、この記録媒体205を別の記録再生装置に装着してもデータの読出し、書きこみが可能な構成としたものである。このように、記録媒体195が複数の記録再生装置において使用可能な構成を持つ図2のような記録再生装置においては記録再生装置ごとに固有のデバイスキーを持つのではなく、複数の記録再生装置に共通な鍵、すなわちシステム全体で共通な鍵をメモリ180に格納する構成とする。

【0082】[データ記録処理およびデータ再生処理]
次に、図1あるいは図2の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図3および図4のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体195に記録する場合においては、図

3 (A) のフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ (デジタルコンテンツ) が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力 I/F 120 に供給されると、ステップ S 301 において、入出力 I/F 120 は、供給されるデジタルコンテンツを受信し、バス 110 を介して、TS 処理手段 300 に出力する。

【0083】TS 処理手段 300 は、ステップ S 302 において、トランスポートストリームを構成する各トランスポートパケットに A TS を付加したブロックデータを生成して、バス 110 を介して、暗号処理手段 150 に出力する。

【0084】暗号処理手段 150 は、ステップ S 303 において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス 110 を介して、ドライブ 190、あるいは記録媒体 I/F 210 に出力する。暗号化コンテンツは、ドライブ 190、あるいは記録媒体 I/F 210 を介して記録媒体 195 に記録 (S 304) され、記録処理を終了する。なお、暗号処理手段 150 における暗号処理については後段で説明する。

【0085】なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む 5 社によって、5CDTCP (Five Company Digital Transmission Content Protection) (以下、適宜、DTCP という) が定められているが、この DTCP では、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ (暗号化コンテンツ) を復号するようになっている。

【0086】この DTCP に規格に基づくデータ送受信においては、データ受信側の入出力 I/F 120 は、ステップ S 301 で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、DTCP に規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段 150 に出力する。

【0087】DTCP によるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

【0088】なお、DTCP によれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキ

ーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、DTCP については、例えば、<http://www.dtcp.com> の URL (Uniform Resource Locator) で特定される Web ページにおいて、インフォメーションバージョン (Informational Version) の取得が可能である。

【0089】次に、外部からのアナログ信号のコンテンツを、記録媒体 195 に記録する場合の処理について、図 3 (B) のフローチャートに従って説明する。アナログ信号のコンテンツ (アナログコンテンツ) が、入出力 I/F 140 に供給されると、入出力 I/F 140 は、ステップ S 321 において、そのアナログコンテンツを受信し、ステップ S 322 に進み、内蔵する A/D、D/A コンバータ 141 で A/D 変換して、デジタル信号のコンテンツ (デジタルコンテンツ) とする。

【0090】このデジタルコンテンツは、MPEG コーデック 130 に供給され、ステップ S 323 において、MPEG エンコード、すなわち MPEG 圧縮による符号化処理が実行され、バス 110 を介して、暗号処理手段 150 に供給される。

【0091】以下、ステップ S 324、S 325、S 326 において、図 3 (A) のステップ S 302、S 303 における処理と同様の処理が行われる。すなわち、TS 処理手段 300 によるトランスポートパケットに対する A TS 付加、暗号処理手段 150 における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体 195 に記録して、記録処理を終了する。

【0092】次に、記録媒体 195 に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図 4 のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図 4 (A) のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ステップ S 401 において、ドライブ 190 または記録媒体 I/F 210 によって、記録媒体 195 に記録された暗号化コンテンツが読み出され、バス 110 を介して、暗号処理手段 150 に出力される。

【0093】暗号処理手段 150 では、ステップ S 402 において、ドライブ 190 または記録媒体 I/F 210 から供給される暗号化コンテンツが復号処理され、復号データがバス 110 を介して、TS 処理手段 300 に出力される。

【0094】TS 処理手段 300 は、ステップ S 403

において、トランスポートストリームを構成する各トランスポートパケットのATSから出力タイミングを判定し、ATSに応じた制御を実行して、バス110を介して、入出力I/F120に供給する。入出力I/F120は、TS処理手段300からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、TS処理手段300の処理、暗号処理手段150におけるデジタルコンテンツの復号処理については後述する。

【0095】なお、入出力I/F120は、ステップS404で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、DTCIPの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

【0096】記録媒体195に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図4(B)のフローチャートに従った再生処理が行われる。

【0097】即ち、ステップS421、S422、S423において、図4(A)のステップS401、S402、S403における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段150において得られた復号されたデジタルコンテンツは、バス110を介して、MPEGコーデック130に供給される。

【0098】MPEGコーデック130では、ステップS424において、デジタルコンテンツがMPEGデコード、すなわち伸長処理が実行され、入出力I/F140に供給される。入出力I/F140は、ステップS424において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換(S425)して、アナログコンテンツとする。そして、ステップS426に進み、入出力I/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【0099】【データフォーマット】次に、図5を用いて、本発明における記録媒体上のデータフォーマットを説明する。本発明における記録媒体上のデータの読み書きの最小単位をブロック(block)という名前と呼ぶ。1ブロックは、 $192 \times X$ (エックス) バイト (例えば $X=32$) の大きさとなっている。

【0100】本発明では、MPEG2のTS (トランスポート・ストリーム) パケット (188バイト) にATSを付加して192バイトとして、それをX個集めて1ブロックのデータとしている。ATSは24乃至32ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp (着信時刻スタンプ) の略である。ATSは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック (セクタ) には、ATSを付加したTS (トランスポート・ストリーム) パケットをX個記録する。本発

明の構成では、トランスポートストリームを構成する各ブロックの第1番目のTSパケットに付加されたATSを用いてそのブロック (セクタ) のデータを暗号化するブロックキーを生成する。

【0101】ランダム性のあるATSを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【0102】なお、図5に示すブロック・シード (Block Seed) は、ATSを含む付加情報である。ブロック・シードは、さらにATSだけでなくコピー制限情報 (CCI: Copy Control Information) も付加した構成としてもよい。この場合、ATSとCCIを用いてブロックキーを生成する構成とすることができる。

【0103】なお、本発明の構成においては、DVD等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図5の最下段に示すように、ブロックの先頭のm (たとえば、 $m=8$ または 16) バイトは暗号化されずに平文 (Unencrypted data) のまま記録され、残りのデータ ($m+1$ バイト以降) が暗号化される。これは暗号処理が8バイト単位としての処理であるために暗号処理データ長 (Encrypted data) に制約が発生するためである。なお、もし暗号処理が8バイト単位でなく、たとえば1バイト単位で行なえるなら、 $m=4$ として、ブロックシード以外の部分をすべて暗号化してもよい。

【0104】【TS処理手段における処理】ここで、ATSの機能について詳細に説明する。ATSは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

【0105】すなわち、例えば複数のTVプログラム (コンテンツ) が多重化されたトランスポートストリームの中から1つまたは幾つかのTVプログラム (コンテンツ) を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる (図7(a) 参照)。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはMPEG2システムズ (ISO/IEC 13818-1) で規定されている仮想的なデコーダであるT-STD (Transport stream System Target Decoder) を破綻させないように符号化時に決定される。

【0106】トランスポートストリームの再生時には、

各トランスポートパケットに付加されたATSによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要がある、トランスポートパケットをDVD等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すATSを付加して記録する。

【0107】図6に、デジタルインタフェース経由で入力されるトランスポートストリームをDVD等の記録媒体であるストレージメディアに記録する時のTS処理手段300において実行する処理を説明するブロック図を示す。端子600からは、デジタル放送等のデジタルデータとしてトランスポートストリームが入力される。図1または図2においては、入出力I/F120を介して、あるいは入出力I/F140、MPEGコーデック130を介して端子600からトランスポートストリームが入力される。

【0108】トランスポートストリームは、ビットストリームパーサ（parser）602に入力される。ビットストリームパーサ602は、入力トランスポートストリームの中からPCR（Program Clock Reference）パケットを検出する。ここで、PCRパケットとは、MPEG2システムズで規定されているPCRが符号化されているパケットである。PCRパケットは、100msec以内の時間間隔で符号化されている。PCRは、トランスポートパケットが受信側に到着する時刻を27MHzの精度で表す。

【0109】そして、27MHz PLL603において、記録再生器が持つ27MHzクロックをトランスポートストリームのPCRにロック（Lock）させる。タイムスタンプ発生回路604は、27MHzクロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード（Block seed）付加回路605は、トランスポートパケットの第1バイト目がスミージングバッファ606へ入力される時のタイムスタンプをATSとして、そのトランスポートパケットに付加する。

【0110】ATSが付加されたトランスポートパケットは、スミージングバッファ606を通過して、端子607から、暗号処理手段150に出力され、後段で説明する暗号処理が実行された後、ドライブ190（図1）、記録媒体I/F210（図2）を介してストレージメディアである記録媒体195に記録される。

【0111】図7は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図7（a）は、ある特定プログラム（コンテンツ）を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図7（a）に示すように不規則なタイミングで現れる。

【0112】図7（b）は、ブロック・シード（Block Seed）付加回路605の出力を示す。ブロック・シード（Block Seed）付加回路605は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示すATSを含むブロック・シード（Block Seed）を付加して、ソースパケットを出力する。図7（c）は記録媒体に記録されたソースパケットを示す。ソースパケットは、図7（c）に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【0113】図8は、記録媒体195に記録されたトランスポートストリームを再生する場合のTS処理手段300の処理構成ブロック図を示している。端子800からは、後段で説明する暗号処理手段において復号されたATS付きのトランスポートパケットが、ブロック・シード（Block seed）分離回路801へ入力され、ATSとトランスポートパケットが分離される。タイミング発生回路804は、再生器が持つ27MHzクロック805のクロックカウンタ値に基づいた時間を計算する。

【0114】なお、再生の開始時において、一番最初のATSが初期値として、タイミング発生回路804にセットされる。比較器803は、ATSとタイミング発生回路804から入力される現在の時刻を比較する。そして、タイミング発生回路804が発生する時間とATSが等しくなった時、出力制御回路802は、そのトランスポートパケットをMPEGコーデック130またはデジタル入出力I/F120へ出力する。

【0115】図9は、入力AV信号を記録再生器100のMPEGコーデック130においてMPEGエンコードして、さらにTS処理手段300においてトランスポートストリームを符号化する構成を示す。従って図9は、図1または、図2におけるMPEGコーデック130とTS処理手段300の両処理構成を併せて示すブロック図である。端子901からは、ビデオ信号が入力されており、それはMPEGビデオエンコーダ902へ入力される。

【0116】MPEGビデオエンコーダ902は、入力ビデオ信号をMPEGビデオストリームに符号化し、それをバッファビデオストリームバッファ903へ出力する。また、MPEGビデオエンコーダ902は、MPEGビデオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ、符号化ビット量、デコードタイムスタンプである。ここで、ピクチャタイプは、I/P/Bピクチャ（picture）の情報である。また、デコードタイムスタンプは、MPEG2システムズで規定されている情報である。

【0117】端子904からは、オーディオ信号が入力されており、それはMPEGオーディオエンコーダ90

5へ入力される。MPEGオーディオエンコーダ905は、入力オーディオ信号をMPEGオーディオストリームに符号化し、それをバッファ906へ出力する。また、MPEGオーディオエンコーダ905は、MPEGオーディオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量、デコードタイムスタンプである。

【0118】多重化スケジューラ908には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ908は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ908は、内部に27MHz精度の基準時刻を発生するクロックを持ち、そして、MPEG2で規定されている仮想的なデコーダモデルであるT-S-TDを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

【0119】パケット符号化制御情報がビデオパケットの場合、スイッチ976はa側になり、ビデオストリームバッファ903からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0120】パケット符号化制御情報がオーディオパケットの場合、スイッチ976はb側になり、オーディオストリームバッファ906から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0121】パケット符号化制御情報がPCRパケットの場合、トランスポートパケット符号化器909は、多重化スケジューラ908から入力されるPCRを取り込み、PCRパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器909へは何も入力されない。

【0122】トランスポートパケット符号化器909は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器909は、間欠的にトランスポートパケットを出力する。到着 (Arrival) タイムスタンプ (time stamp) 計算手段910は、多重化スケジューラ908から入力されるPCRに基づいて、トランスポートパケットの第1バイト目が受

信側に到着する時刻を示すATSを計算する。

【0123】多重化スケジューラ908から入力されるPCRは、MPEG2で規定されるトランスポートパケットの10バイト目の受信側への到着時刻を示すので、ATSの値は、PCRの時刻から10バイト前のバイトが到着する時刻となる。

【0124】ブロック・シード (Block Seed) 付加回路911は、トランスポートパケット符号化器909から出力されるトランスポートパケットにATSを付加する。ブロック・シード (Block seed) 付加回路911から出力されるATS付きのトランスポートパケットは、スムージングバッファ912を通して、暗号処理手段150へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体195へ格納される。

【0125】記録媒体195へ格納されるATS付きのトランスポートパケットは、暗号処理手段150で暗号化される前に図7(c)に示すように間隔を詰めた状態で入力され、その後、記録媒体195に格納される。トランスポートパケットが間隔を詰めて記録されても、ATSを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

【0126】ところで、ATSの大きさは32ビットに決まっているわけではなく、24ビット乃至31ビットでも構わない。ATSのビット長が長いほど、ATSの時間カウンタが一周する周期が長くなる。例えば、ATSが27MHz精度のバイナリーカウンタである場合、24-bit長のATSが一周する時間は、約0.6秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、MPEG2の規定により、最大0.1秒と決められているからである。しかしながら、十分な余裕を見て、ATSを24-bit以上にしても良い。

【0127】このように、ATSのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図10に示す。図10の例1は、ATSを32ビット分使用する例である。図10の例2は、ATSを30ビットとし、コピー制御情報 (CCI) を2ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、SCMS: Serial Copy Management SystemやCGMS: Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー (Copy Free)、1世代のみのコピーを許可する1世代コピー許可 (One Generation Copy Allowed)、コピーを認めないコピー禁止 (Copy Prohibited) などの情報が表せる。

【0128】図10に示す例3は、ATSを24ビットとし、CCIを2ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン (Macrovision) のオン/オフ (On/Off) を示す情報など、様々な情報を利用することが可能である。

【0129】[記録データの互換性が必要なシステムにおけるデータ記録処理に伴う暗号処理] 次に、記録データの互換性が必要なシステム、すなわち、ある記録再生器において記録した記録媒体を他の記録再生器において再生可能とすることが要請されるシステムでのデータ記録処理に伴う暗号処理について説明する。記録データの互換性が必要なシステムは例えば図2に示すような記録再生装置200であり、記録媒体195が他の記録再生器においても使用可能とする要請があるものである。

【0130】このようなシステムにおけるデータ記録処理における暗号化処理について、図11、図12の処理ブロック図および図13のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例は、特開平11-224461号公報 (特願平10-25310号) に記載した構成と同様に、ある記録再生装置で記録したデータを、別の記録再生装置で再生することが必要な、すなわち記録データの互換性が必要なシステムである。そして、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクID (Disc ID) を、データを暗号化する鍵に作用させるようにしている。

【0131】図11、図12の処理ブロック図に従って、暗号処理手段150が実行するデータの暗号化処理の概要について説明する。

【0132】記録再生装置1100は自身のメモリ180 (図2参照) に格納しているマスターキー1101を読み出す。マスターキー1101は、ライセンスを受けた記録再生装置に格納された秘密キーであり、複数の記録再生装置に共通なキー、すなわちシステム全体で共通なキーである。記録再生装置1100は例えば光ディスクである記録媒体1120に識別情報としてのディスクID (Disc ID) 1103が既に記録されているかどうかを検査する。記録されていれば、ディスクID (Disc ID) 1103を読み出し (図11に相当)、記録されていないか、暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクID (Disc ID) 1201を生成し、ディスクに記録する (図12に相当)。ディスクID (Disc ID) 1103はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【0133】記録再生装置1100は、次にマスターキーとディスクIDを用いて、ディスク固有キー (Disc Unique Key) を生成1102する。ディスク固有キー (Dis

c Unique Key) の具体的な生成方法としては、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。

【0134】次に、記録ごとの固有鍵であるタイトルキー (Title Key) を暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成1104し、ディスク1120に記録する。ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキーを格納することができる。

【0135】次にディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) から、タイトル固有キー (Title Unique Key) を生成する。この生成の具体的な方法も、上記のように、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法など、いくつか挙げることができる。

【0136】なお、上記の説明では、マスターキー (Master Key) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とディスクID (Disc ID) とタイトルキー (Title Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マスターキー (Master Key) とディスクID (Disc ID) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0137】ところで、たとえば上記の5CDTCPに規定される伝送フォーマットのひとつを使用した場合、データはMPEG2のTSパケットで伝送される場合がある。たとえば、衛星放送を受信したセットトップボックス (STB: Set Top Box) がこの放送を記録機に5CDTCPを用いて伝送する際に、STBは衛星放送通信路で伝送されたMPEG2 TSパケットをIEEE 1394上も伝送することが、データ変換の必要がなく望ましい。

【0138】記録再生装置1100は記録すべきコンテンツデータをこのTSパケットの形で受信し、前述したTS処理手段300において、各TSパケットを受信した時刻情報であるATSを付加する。なお、先に説明したように、ブロックデータに付加されるブロック・シードは、ATSとコピー制御情報、さらに他の情報を組み

合わせた値から構成してもよい。

【0139】ATSを付加したTSパケットをX個（例えば $X=32$ ）並べて、1ブロックのブロックデータが形成（図5の上の図参照）され、図11、12の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第1～4バイトが分離され（セクタ1108）て出力される32ビットのATSを含むブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成1107される。

【0140】ブロック・キー（Block Key）の生成方法の例を図14に示す。図14では、いずれも32ビットのブロック・シード（Block Seed）と、64ビットのタイトル固有キー（Title Unique Key）とから、64ビットのブロックキー（Block Key）を生成する例を2つ示している。

【0141】上段に示す例1は、鍵長64ビット、入出力がそれぞれ64ビットの暗号関数を使用している。タイトル固有キー（Title Unique Key）をこの暗号関数の鍵とし、ブロックシード（Block Seed）と32ビットの定数（コンスタント）を連結した値を入力して暗号化した結果をブロックキー（Block Key）としている。

【0142】例2は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー（Title Unique Key）とブロックシード（Block Seed）を連結した値をSHA-1に入力し、その160ビットの出力を、たとえば下位64ビットのみ使用するなど、64ビットに縮約したものをブロックキー（Block Key）としている。

【0143】なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）とディスクID（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）を用いてブロックキー（Block Key）を生成してもよい。

【0144】ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図11、12の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第1～mバイト（たとえば $m=8$ バイト）は分離（セクタ1108）されて暗号化対象とせず、 $m+1$ バイト目から最終データまでを暗号化1109する。なお、暗号化されないmバイト中にはブロック・シードとしての第1～4バイトも含まれる。セクタ1108により分離された第 $m+1$ バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化1109される。暗号化アルゴリズムとし

ては、たとえばFIPS 46-2で規定されるDES（Data Encryption Standard）を用いることができる。

【0145】ここで、使用する暗号アルゴリズムのブロック長（入出力データサイズ）がDESのように8バイトであるときは、Xを例えば32とし、mを例えば8の倍数とすることで、端数なく $m+1$ バイト目以降のブロックデータ全体が暗号化できる。

【0146】すなわち、1ブロックに格納するTSパケットの個数をX個とし、暗号アルゴリズムの入出力データサイズをLバイトとし、nを任意の自然数とした場合、 $192 * X = m + n * L$ が成り立つようにX、m、Lを定めることにより、端数処理が不要となる。

【0147】暗号化した第 $m+1$ バイト以降のブロックデータは暗号処理のされていない第1～mバイトデータとともにセクタ1110により結合されて暗号化コンテンツ1112として記録媒体1120に格納される。

【0148】以上の処理により、コンテンツはブロック単位でATSを含むブロック・シードに基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納されることになる。先にも説明したようにATSはブロック固有のランダム性の高いデータであるので、各ブロックに設定されたATSに基づくブロック鍵は、それぞれが異なった鍵となる。すなわち、ブロック毎に暗号鍵が変更され、このため暗号解析に対する強度を高めることができる。また、ブロック・シードを暗号鍵生成データとして使用することにより、ブロックごとの暗号鍵をデータと別に保存しておく必要がなく、そのため暗号鍵の保存領域が不要となり記憶領域を節約できる。また、ブロック・シードはコンテンツデータとともに書き込み読み出しが実行されるデータであるので、従来のように暗号鍵を別領域に保存する構成とは異なり、記録再生時に暗号鍵データを書きこんだり読み出したりする処理が省略でき効率的な処理が可能となる。

【0149】次に図13に示すフローチャートに従って、データ記録処理にともなって実行されるTS処理手段300におけるATS付加処理および暗号処理手段150における暗号処理の処理の流れを説明する。図13のS1301において、記録再生装置は自身のメモリ180に格納しているマスターキーを読み出す。

【0150】S1302において、記録媒体に識別情報としてのディスクID（Disc ID）が既に記録されているかどうかを検査する。記録されていればS1303でこのディスクIDを読み出し、記録されていなければS1304で、ランダムに、もしくはあらかじめ定められた方法でディスクIDを生成し、ディスクに記録する。次に、S1305では、マスターキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用する

ことで求める。

【0151】次にS1306に進み、その一回の記録ごとの固有の鍵としてタイトルキー (Title Key) を生成しディスクに記録する。次にS1307で、上記のディスク固有キーとタイトルキーから、タイトル固有キーを生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法を適用する。

【0152】S1308では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S1309で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S1310で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS1311に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0153】次に、暗号処理手段150は、S1312で、ブロックデータの先頭の32ビット (ATSを含むブロック・シード) とS1307で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【0154】S1313では、ブロックキーを用いてS1311で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるDES (Data Encryption Standard) が適用される。

【0155】S1314で、暗号化したブロックデータを記録媒体に記録する。S1315で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS1308に戻って残りのデータの処理を実行する。

【0156】[記録データの互換性が必要なシステムにおけるデータ再生処理に伴う暗号処理] 次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図15の処理ブロック図と、図16のフローチャートを用いて説明する。

【0157】まず、図15に示す処理ブロック図に従って説明する。記録再生装置1500はディスク1520からディスクID1502を、また自身のメモリからマスターキー1501を読み出す。先の記録処理の説明から明らかなように、ディスクIDはディスクに記録されているか、記録されていない場合は記録再生器において生成してディスクに記録したディスク固有の識別子であ

る。マスターキー1501は、ライセンスを受けた記録再生装置に格納された秘密キーである。

【0158】記録再生装置1500は、次に、ディスクID (Disc ID) とマスターキー (Master Key) を用いてディスク固有キー (Disc Unique Key) を生成1503する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。

【0159】次に、ディスクから読み出すべきデータに対応して記録されたタイトルキー (Title Key) 1504を読み出し、タイトルキー (Title Key) 1504とディスク固有キー (Disc Unique Key) からタイトル固有キー (Title Unique Key) を生成1505する。この生成方法も、ハッシュ関数SHA-1、ブロック暗号関数を用いたハッシュ関数の適用が可能である。

【0160】なお、上記の説明では、マスターキー (Master Key) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とディスクID (Disc ID) とタイトルキー (Title Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マスターキー (Master Key) とディスクID (Disc ID) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0161】次にディスクに格納されている暗号化コンテンツ1507から順次ブロックデータ (Block Data) を読み出し、ブロックデータ (Block Data) の先頭の4バイトを構成するブロック・シード (Block Seed) をセレクタ1508において分離して、タイトル固有キー (Title Unique Key) との相互処理により、ブロックキー (Block Key) を生成する。

【0162】ブロック・キー (Block Key) の生成方法は、先に説明した図14の構成を適用することができる。すなわち、32ビットのブロック・シード (Block Seed) と、64ビットのタイトル固有キー (Title Unique Key) とから、64ビットのブロックキー (Block Key) を生成する構成が適用できる。

【0163】なお、上記ではディスク固有キー (Disc Unique key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー (Disc Uni

que Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとにマスターキー (Master Key) とディスク ID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) を用いてブロックキー (Block Key) を生成してもよい。

【0164】ブロックキーが生成されると、ブロックキー (Block Key) を用いて暗号化されているブロックデータを復号1509し、セクタ1510を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにATSが付加されており、先に説明したTS処理手段300において、ATSに基づくストリーム処理が実行される。その後、データは、使用、たとえば、画像を表示したり、音楽を鳴らしたりすることが可能となる。

【0165】このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でATSを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。

【0166】次に図16に示すフローチャートに従って、復号処理および再生処理について、処理の流れを説明する。図16のS1601において、記録再生装置はディスクからディスクIDを、また自身のメモリからマスターキーを読み出す。S1602で、ディスクIDとマスターキーを用いてディスク固有キーを生成する。

【0167】次にS1603で、ディスクから読み出すべきデータのタイトルキーを読み出し、S1604で、タイトルキーとディスク固有キーからタイトル固有キーを生成する。次にS1605でディスクから暗号化されて格納されているブロックデータを読み出す。S1606で、ブロックデータの先頭の4バイトのブロックシード (Block Seed) と、S1604で生成したタイトル固有キーを用いてブロックキーを生成する。

【0168】次に、S1607で、ブロックキーを用いて暗号化されているブロックデータを復号し、S1608で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければS1605に戻り残りのデータを読み出す。

【0169】[記録されたデータの互換性が不要ないシステムにおけるデータ記録処理に伴う暗号処理] 次に、記録データの互換性が不要ないシステム、すなわち、ある記録再生器において記録した記録媒体を他の記録再生器において再生可能とすることが要請されないシステム、すなわち、記録データはそれを記録した装置でのみ読み出しができればよいシステムでのデータ記録処理に伴う暗号処理について図17の処理ブロック図および図18のフローチャートを用いて説明する。

【0170】図17の処理ブロック図を参照しながら、図18のフローチャートの処理手順に従って順次説明する。

【0171】まず、図18のS1801において、記録

再生装置1700 (図17参照) は、その装置固有の鍵であるデバイス固有キー (Device Unique Key) を生成する。

【0172】図17に示すようにデバイス固有キー (Device Unique Key) の生成はLSIキー、デバイスキー、メディアキー、ドライブキーのいずれか、またはこれらの任意の組合わせデータに基づいて生成する。LSIキーは、暗号処理手段150 (図1参照) を構成するLSIに対してLSIの製造時に格納されたキーである。デバイス・キーは記録再生器の製造時にフラッシュメモリ、EEPROM等の記憶素子に格納されたデバイスすなわち記録再生器に対応して設定されたキーである。メディアキーはコンテンツを格納する記録媒体に対して設定され記録媒体に格納されたキーである。ドライブキーは、DVDドライブ等、記録媒体のドライブ装置に対して付与されたキーである。

【0173】本実施例では、デバイス固有キー (Device Unique Key) を、LSIキー、デバイスキー、メディアキー、ドライブキーのいずれか、またはこれらの任意の組合わせデータに基づいて生成する。

【0174】例えば、LSIキーとデバイスキーを使用したデバイス固有キーの生成処理について図19を用いて説明する。図19は、例えば図1の暗号処理手段150をLSIとして構成した暗号処理手段LSI1900における処理例を示している。

【0175】LSIキー記憶部1901は、複数の暗号処理手段LSIに共通 (従って、複数の記録再生装置にも共通) のLSIキーを記憶している。具体的には例えば、LSI製造時のロット毎に一律のキーが格納される。また、すべての暗号処理手段LSIに共通のLSIキーを記憶する構成としてもよいし、幾つかの暗号処理手段LSIのグループごとに共通のLSIキーを記憶するようにしても良い。LSIキーを、幾つの暗号処理手段LSIに共通とするかは、例えば、暗号処理手段LSIの製造コストとの関係で決めることができる。

【0176】暗号処理手段LSI1900の鍵生成部は、キー記憶部1901に記憶されているLSIキーを読み出すとともに、暗号処理手段LSI1900の外部の記憶素子としての例えば記録再生装置のROMに記憶されているデバイスキー1910を、バスを介して読み出すことで取得し、このLSIキーおよびデバイスキーに対して、キーを生成するための関数 (鍵生成関数) を適用して、デバイス固有キー (Device Unique Key) を生成1902する。

【0177】なお、鍵生成関数としては、LSIキーおよびデバイスキーから、デバイス固有キー (Device Unique Key) を計算することは容易であるが、その逆に、デバイス固有キー (Device Unique Key) から、LSIキーやデバイスキーを計算することはできない一方向性関数を用いることができる。具体的には、デバイス固有

キー生成部1902は、例えば、FIPS180-1のSHA-1ハッシュ関数等の一方方向性関数に対して、LSIキーとデバイスキーとを連結したものを入力として与えて、そのハッシュ関数を演算することにより、デバイス固有キー(Device Unique Key)を生成する。デバイス固有キー(Device Unique Key)は、例えば、FIPS46-2、FIPS46-3のDES、Triple-DES等を利用した一方方向性関数を用い、LSIキーで、デバイスキーを暗号化することにより求めてもよい。

【0178】このようにして得られたデバイス固有キー(Device Unique Key)と、コンテンツデータの付加データとして設定されたブロック・シードとによりブロックキーを生成して、生成したブロックキーに基づいて暗号化処理または復号処理を実行して暗号化コンテンツ1906の記録媒体1920に対する格納処理、あるいは暗号化コンテンツ1906の記録媒体1920からの再生処理を実行する。

【0179】コンテンツを暗号化方式、および復号方式としては、例えば、FIPS46-2に挙げられているデータ・エンクリプション・スタンダード(Data Encryption Standard)その他を用いることが可能である。

【0180】図19は、LSIキーおよびデバイスキーから、デバイス固有キー(Device Unique Key)を生成する例であるが、例えば、記録媒体に固有の値としてのメディアキーが割り当てられている場合や、記録媒体のドライブに対する固有の値としてのドライブキーが割り当てられている場合には、デバイス固有キー(Device Unique Key)の生成に、そのメディアキーやドライブキーも用いることが可能である。

【0181】デバイス固有キー(Device Unique Key)を、LSIキーおよびデバイスキーの他に、メディアキーおよびドライブキーのすべてを用いて生成する場合の処理構成例を図20に示す。図20は、ISO/IEC9797で規定されているデータインテグリティメカニズム(DIM: Data Integrity Mechanism)によって、デバイス固有キー(Device Unique Key)を生成する処理構成例を示している。

【0182】暗号化部2001は、LSIキーを、デバイスキーで暗号化し、演算器2004に出力する。演算器2004は、暗号化部2001の出力と、メディアキーとを排他的論理和し、暗号化部2002に供給する。暗号化部2002は、LSIキーを鍵とし、演算器2004の出力を暗号化し、演算器2005に出力する。演算器2005は、暗号化部2002の出力と、ドライブキーとを排他的論理和し、暗号化部2003に出力する。暗号化部2003は、LSIキーを鍵とし、演算器2005の出力を暗号化し、その暗号化結果を、デバイス固有キー(Device Unique Key)として出力する。

【0183】図18に戻り、データ記録処理ステップの説明を続ける。ステップS1801では、上述のように

LSIキー、デバイスキー、メディアキー、ドライブキーのいずれか、またはこれらの任意の組み合わせデータに基づいてデバイス固有キーを生成する。

【0184】S1802では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S1803で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S1804で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS1805に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0185】次に、S1806で、暗号処理手段150は、ブロックデータの先頭の32ビット(ATSを含むブロック・シード)とS1801で生成したデバイス固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【0186】S1807では、ブロックキーを用いてS1805で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるDES(Data Encryption Standard)が適用される。

【0187】S1808で、暗号化したブロックデータを記録媒体に記録する。S1809で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS1802に戻って残りのデータの処理を実行する。

【0188】[記録されたデータの互換性が不要ないシステムにおけるデータ再生処理に伴う暗号処理] 次に、このようにして記録されたデータの再生処理について、図21の処理ブロック図および図22のフローチャートを用いて説明する。

【0189】図21の処理ブロック図を参照しながら、図22のフローチャートの処理手順に従って順次説明する。

【0190】まず、図22のS2201において、記録再生装置2100(図21参照)は、その装置固有の鍵であるデバイス固有キー(Device Unique Key)を生成する。

【0191】図21に示すようにデバイス固有キー(Device Unique Key)の生成はLSIキー、デバイスキー、メディアキー、ドライブキーのいずれか、またはこれらの任意の組み合わせデータに基づいて生成2101する。ここで各キーは先に説明した通り、LSIキーは、

暗号処理手段150(図1、図2参照)を構成するLSIに対してLSIの製造時に格納されたキー、デバイス・キーは記録再生器の製造時にフラッシュメモリ、EEPROM等の記憶素子に格納されたデバイスに対応して設定されたキー、メディアキーはコンテンツを格納する記録媒体に対して設定され記録媒体に格納されたキー、ドライブキーは、DVDドライブ等、記録媒体のドライブ装置に対して付与されたキーである。

【0192】次にS2202でディスクから暗号化されて格納されているブロックデータを読み出す。S2203で、ブロックデータの先頭の4バイトのブロックシード(Block Seed)と、S2201で生成したデバイス固有キーを用いてブロックキーを生成(図21の2102)する。

【0193】次に、S2204で、ブロックキーを用いて暗号化されているブロックデータを復号(図21の2105)し、S2205で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければS2202に戻り残りのデータを読み出す。

【0194】なお、この処理においても記録媒体2120に格納された暗号化コンテンツ2103はブロックデータの先頭第1~4バイトのブロックシードがセクタ2104において分離され、また暗号化されていない第1~mバイトデータは、復号処理を実行されずに、セクタ2106において結合されて出力される。復号データには、パケット毎に入力タイミングを表すATS(Arrival Time Stamp: 着信時刻スタンプ)が付加されており、前述のTS処理手段における処理により正常な再生が可能となる。

【0195】このように、本発明の構成では、ブロックデータの先頭のTSパケットの受信時刻によって変化するATSに基づいて変化するブロックキーによって、コンテンツを暗号化するようにしたので、仮に、あるコンテンツの暗号化に用いたブロックキーが漏洩しても、他のコンテンツの保護に影響はない。従来のシステムのようにひとつの暗号鍵をすべてのコンテンツの暗号化に使用した場合、コンテンツが、常に、固定のデータキーによって暗号化されるため、例えば、ある平文のコンテンツと、それを、データキーによって暗号化した暗号文のコンテンツとの組が、違法コピーを行おうとする者に入手された場合に、いわゆる線形攻撃や差分攻撃といった暗号攻撃法を用いて、データキーが解読され、これにより、そのデータキーによって暗号化した暗号化コンテンツすべてが復号され、違法にコピーされるおそれがあるが、本発明の構成では、各ブロック単位で暗号鍵が異なるため、このような自体の発生する可能性はほとんどない。

【0196】本発明の構成では、ひとつの暗号鍵で暗号化されるデータの量が1ブロックであり、極めて少ないデータ量であるため、いわゆる線形攻撃や差分攻撃とい

った暗号攻撃法を用いて鍵を求めることが非常に困難になる。

【0197】さらに、本発明の構成では、本来のデータの付加情報として設定されるATSに基づいて暗号鍵を生成しているため、ブロックごとに暗号鍵を変化させる構成としても、その暗号鍵を記録媒体のデータセクタのセクタヘッダ部などに新たに記録する必要がないため、余分な記録容量を消費せず、また記録、再生時にブロックごとの暗号鍵のリード、ライトなどの処理を行う必要がない。

【0198】[記録されたデータ再生についての機器制限の設定が可能なシステムにおけるデータ暗号化および記録処理] 上述の構成は、マスターキーによりブロックキーを生成可能とした構成であり、共通のマスターキーを有する記録再生器においては、再生が可能となる。しかし、ある特定のデータについては、データ記録を実行したその記録再生器でのみ再生可能としたい場合がある。以下では、このような機器制限の設定を実行する構成について説明する。

【0199】本例は、例えば先に説明した図1、図2の記録再生器において記録媒体195が着脱可能であり、記録媒体195を他の記録再生器にも装着可能な構成において効果的なシステムである。すなわち、記録媒体195に対してデータを記録したとき、その記録データを記録した記録媒体を他の記録再生器に装着した場合に再生可能とするか再生不可能とするかを設定可能としたものである。

【0200】このようなシステムにおけるデータ記録処理における暗号化処理について、図23、図24の処理ブロック図および図25のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクID(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

【0201】図23、図24の処理ブロック図に従って、暗号処理手段150が実行するデータの暗号化処理の概要について説明する。

【0202】記録再生装置2300は自身のメモリ180(図1、2参照)に格納しているマスターキー2301、デバイス識別子としてのデバイスID2331、デバイス固有キー2332を読み出す。マスターキー2301は、ライセンスを受けた記録再生装置に格納された秘密キーであり、複数の記録再生装置に共通なキー、すなわちシステム全体で共通なキーである。デバイスIDは記録再生装置2300の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイスIDは公開されていてもよい。デバイス固有キーは、その記録再生器2300に固有の秘密鍵であり、予め個々の記録再生装置に応じて異なるように

設定されて格納されたキーである。これらは予め記録再生装置2300のメモリに格納されている。

【0203】記録再生装置2300は例えば光ディスクである記録媒体2320に識別情報としてのディスクID (Disc ID) 2303が既に記録されているかどうかを検査する。記録されていれば、ディスクID (Disc ID) 2303を読み出し(図23に相当)、記録されていなければ、暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクID (Disc ID) 2401を生成し、ディスクに記録する(図24に相当)。ディスクID (Disc ID) 2303はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【0204】記録再生装置2300は、次にマスターキーとディスクIDを用いて、ディスク固有キー(Disc Unique Key)を生成2302する。ディスク固有キー(Disc Unique Key)の具体的な生成方法としては、図26に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー(Master Key)とディスクID (Disc ID)を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー(Disc Unique Key)として使用する例2の方法が適用できる。

【0205】次に、記録ごとの固有鍵であるタイトルキー(Title Key)を暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成2304し、ディスク2320に記録する。

【0206】さらに、このタイトル(データ)がデータ記録を実行した記録再生装置でのみ再生可能とする(機器制限あり)か、他の機器においても再生可能とする(再生機器制限なし)のいずれであるかを示すフラグ、すなわち再生機器制限フラグ(Player Restriction Flag)を設定し2333、ディスク2320に記録する2335。さらに、機器識別情報としてのデバイスIDを取り出して2331、ディスク2320に記録する2334。

【0207】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー2305、再生機器制限フラグ2335、デバイスID2334を格納することができる。

【0208】次にディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスID、あるいは、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイス固有キー、いずれかの組合せから、タイトル固有キー(Title Unique Key)を生成する。

【0209】すなわち、再生機器制限をしない場合には、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスIDとからタイトル固有キー(Title Unique Key)を生成し、再生機器制限をする場合には、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイス固有キーとからタイトル固有キー(Title Unique Key)を生成する。

【0210】このタイトル固有キー(Title Unique Key)生成の具体的な方法は、図28に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー(Title Key)とディスク固有キー(Disc Unique Key)と、デバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID)とデバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー(Title Unique Key)として使用する例2の方法が適用できる。

【0211】なお、上記の説明では、マスターキー(Master Key)とディスクID (Disc ID)からディスク固有キー(Disc Unique Key)を生成し、これとタイトルキー(Title Key)とデバイスID、もしくはタイトルキー(Title Key)とデバイス固有キーからタイトル固有キー(Title Unique Key)をそれぞれ生成するようにしているが、ディスク固有キー(Disc Unique Key)を不要としてマスターキー(Master Key)とディスクID (Disc ID)とタイトルキー(Title Key)と、デバイスIDもしくはデバイス固有キーから直接タイトル固有キー(Title Unique Key)を生成してもよく、また、タイトルキー(Title Key)を用いずに、マスターキー(Master Key)とディスクID (Disc ID)と、デバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)からタイトル固有キー(Title Unique Key)相当の鍵を生成してもよい。

【0212】たとえば上記の5CDTCPに規定される伝送フォーマットのひとつを使用した場合、データはMPEG2のTSパケットで伝送される場合がある。たとえば、衛星放送を受信したセットトップボックス(STB: Set Top Box)がこの放送を記録機に5CDTCPを用いて伝送する際に、STBは衛星放送通信路で伝送されたMPEG2 TSパケットをIEEE1394上も伝送することが、データ変換の必要がなく望ましい。

【0213】記録再生装置2300は記録すべきコンテンツデータをこのTSパケットの形で受信し、前述したTS処理手段300において、各TSパケットを受信した時刻情報であるATSを付加する。なお、先に説明したように、ブロックデータに対する付加情報としてのプ

ロック・シードとしてATSとコピー制御情報、さらに他の情報を組み合わせた値を付加する構成としてもよい。

【0214】ATSを付加したTSパケットをX個（例えばX=32）並べて、1ブロックのブロックデータが形成（図5の上の図参照）され、図23、24の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第1～4バイトが分離され（セクタ1108）て出力される32ビットのATSを含むブロックシード（Block Seed）と、先に生成したタイトル固有キー（Title Unique Key）とから、そのブロックのデータを暗号化する鍵であるブロック・キー（Block Key）が生成2307される。ブロック・キー（Block Key）の生成方法は先に説明した図14の方法が適用可能である。

【0215】なお、上記ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）とディスクID（Disc ID）とタイトルキー（Title Key）とブロックシード（Block Seed）と、デバイスID（再生機器制限をしない場合）もしくはデバイス固有キー（再生機器制限をする場合）を用いてブロックキー（BlockKey）を生成してもよい。

【0216】ブロックキーが生成されると、生成されたブロックキー（Block Key）を用いてブロックデータを暗号化する。図23、24の下段に示すように、ブロックシード（Block Seed）を含むブロックデータの先頭の第1～mバイト（たとえばm=8バイト）は分離（セクタ2308）されて暗号化対象とせず、m+1バイト目から最終データまでを暗号化2309する。なお、暗号化されないmバイト中にはブロック・シードとしての第1～4バイトも含まれる。セクタ2308により分離された第m+1バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化2309される。暗号化アルゴリズムとしては、たとえばFIPS 46-2で規定されるDES（Data Encryption Standard）を用いることができる。

【0217】ここで、使用する暗号アルゴリズムのブロック長（入出力データサイズ）がDESのように8バイトであるときは、Xを例えば32とし、mを例えば8の倍数とすることで、端数なくm+1バイト目以降のブロックデータ全体が暗号化できる。

【0218】すなわち、1ブロックに格納するTSパケットの個数をX個とし、暗号アルゴリズムの入出力データサイズをLバイトとし、nを任意の自然数とした場合、 $192 * X = m + n * L$ が成り立つようにX、m、Lを定めることにより、端数処理が不要となる。

【0219】暗号化した第m+1バイト以降のブロックデータは暗号処理のされていない第1～mバイトデータとともにセクタ2310により結合されて暗号化コンテンツ2312として記録媒体1120に格納される。

【0220】以上の処理により、コンテンツはブロック単位でATSを含むブロック・シードに基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。また、ブロック鍵は、再生機器制限をしない場合は、デバイスIDに基づいて生成され、再生機器制限をする場合は、デバイス固有キーに基づいて生成される。これらの暗号化データは、再生機器制限をした場合は、そのデータを記録した機器でのみ再生可能となる。

【0221】すなわち、再生機器制限なしの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイスIDを含むデータに基づいて生成されるとともに、デバイスIDが記録媒体に格納される。従って、記録媒体を再生しようとする機器は、記録媒体からデバイスIDを取得可能であり、同様のブロックキーを生成することが可能となるのでブロックデータの復号が可能となる。しかし、再生機器制限ありの場合は、ブロックデータの暗号化鍵であるブロックキーが、デバイス固有キーを含むデータに基づいて生成される。このデバイス固有キーはデバイス毎に異なる秘密鍵であり、他の機器は、そのキーを取得することはできない。また、ブロックデータを暗号化して記録媒体に格納する場合、デバイス固有キーの記録媒体に対する書き込み処理は実行されない。従って、他の再生機器では、暗号化されたブロックデータを格納した記録媒体を装着しても、同一のデバイス固有キーを取得することができないので、ブロックデータを復号するための復号キーを生成することができず、復号不可能となり再生できない。なお、再生処理の詳細については後述する。

【0222】次に図25に示すフローチャートに従って、データ記録処理にともなって実行されるTS処理手段300におけるATS付加処理および暗号処理手段150における暗号処理の処理の流れを説明する。図25のS2501において、記録再生装置は自身のメモリ180に格納しているマスターキー、デバイス識別子としてのデバイスID、デバイス固有キーを読み出す。

【0223】S2502において、記録媒体に識別情報としてのディスクID（Disc ID）が既に記録されているかどうかを検査する。記録されていればS2503でこのディスクIDを読み出し、記録されていなければS2504で、ランダムに、もしくはあらかじめ定められた方法でディスクIDを生成し、ディスクに記録する。次に、S2505では、マスターキーとディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用する

ことで求める。

【0224】次にS2506に進み、その一回の記録ごとの固有の鍵としてのタイトルキー (Title Key)、再生機器制限フラグ (Player Restriction Flag)、さらに、機器識別情報としてのデバイスIDを取り出してディスクに記録する。次にS2507で、上記のディスク固有キーとタイトルキーと、デバイスID (再生機器制限をしない場合) もしくはデバイス固有キー (再生機器制限をする場合) から、タイトル固有キーを生成する。

【0225】タイトル固有キーの生成の詳細フローを図27に示す。暗号処理手段150は、ステップS2701において、再生機器制限をするかしないかの判定を実行する。この判定は、記録再生器を使用するユーザによって入力された指示データ、あるいはコンテンツに付加された利用制限情報に基づいて判定する。

【0226】S2701の判定がNo、すなわち、再生機器制限をしない場合は、ステップS2702に進み、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイスIDとから、タイトル固有キー (Title Unique Key) を生成する。

【0227】S2701の判定がYes、すなわち、再生機器制限をする場合は、ステップS2703に進みディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイス固有キーとから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【0228】S2508では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S2509で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S2510で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS2511に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0229】次に、暗号処理手段150は、S2512で、ブロックデータの先頭の32ビット (ATSを含むブロック・シード) とS2507で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【0230】S2513では、ブロックキーを用いてS2511で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規

定されるDES (Data Encryption Standard) が適用される。

【0231】S2514で、暗号化したブロックデータを記録媒体に記録する。S2515で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS2508に戻って残りのデータの処理を実行する。

【0232】[記録されたデータ再生についての機器制限の設定が可能なシステムにおけるデータ復号および再生処理] 次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図29の処理ブロック図と、図30のフローチャートを用いて説明する。

【0233】まず、図29に示す処理ブロック図に従って説明する。記録再生装置2900はディスク2920からディスクID2902を、また自身のメモリからマスターキー2901、デバイス識別子としてのデバイスID2931、デバイス固有キー2932を読み出す。先の記録処理の説明から明らかなように、ディスクIDはディスクに記録されているか、記録されていない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。マスターキー2901は、ライセンスを受けた記録再生装置に格納された秘密キーであり、デバイスIDは記録再生装置2900固有の識別子、デバイス固有キーは、その記録再生器に固有の秘密鍵である。

【0234】記録再生装置2900は、次に、ディスクID (Disc ID) とマスターキー (Master Key) を用いてディスク固有キー (Disc Unique Key) を生成2903する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。

【0235】次に、ディスクから読み出すべきデータに対応して記録されたタイトルキー (Title Key) 2905を読み出し、さらに、このデータを記録した記録再生器のデバイスID2935と、データに対応して設定された再生機器制限フラグ2934を読み出し、読み出した再生機器制限フラグ2933が示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスID2935と自己のデバイスID2931が一致する」か、あるいは、読み出した再生機器制限フラグ2933が示す再生機器制限情報が、「再生機器制限なし」である場合は、再生可能となり、読み出した再生機器制限フラグ2933が示す再生機器制限情報

が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスID 2934と自己のデバイスID 2931が一致しない」場合は、再生不可能となる。

【0236】再生不可能とされる場合は、データは、そのデータを記録した記録再生器固有のデバイス固有キーに基づいて生成されたブロックキーによって暗号化されており、そのデータを記録した記録再生器以外の記録再生器は同一のデバイス固有キーを保有しないので、データを復号するためのブロックキーを生成することができない場合である。

【0237】再生可能である場合は、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスID、あるいは、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイス固有キー、いずれかの組合せから、タイトル固有キー(Title Unique Key)を生成する。

【0238】すなわち、再生機器制限をしない設定である場合には、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、デバイスIDとからタイトル固有キー(Title Unique Key)を生成し、再生機器制限をする設定である場合には、ディスク固有キー(Disc Unique Key)とタイトルキー(Title Key)と、自己のデバイス固有キーとからタイトル固有キー(Title Unique Key)を生成する。このキー生成方法としては、ハッシュ関数SHA-1、ブロック暗号関数を用いたハッシュ関数の適用が可能である。

【0239】なお、上記の説明では、マスターキー(Master Key)とディスクID(Disc ID)からディスク固有キー(Disc Unique Key)を生成し、これとタイトルキー(Title Key)とデバイスID、もしくはタイトルキー(Title Key)とデバイス固有キーからタイトル固有キー(Title Unique Key)をそれぞれ生成するようにしているが、ディスク固有キー(Disc Unique Key)を不要としてマスターキー(Master Key)とディスクID(Disc ID)とタイトルキー(Title Key)と、デバイスIDもしくはデバイス固有キーから直接タイトル固有キー(Title Unique Key)を生成してもよく、また、タイトルキー(Title Key)を用いずに、マスターキー(Master Key)とディスクID(Disc ID)と、デバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)からタイトル固有キー(Title Unique Key)相当の鍵を生成してもよい。

【0240】次にディスクに格納されている暗号化コンテンツ2912から順次ブロックデータ(Block Data)を読み出し、ブロックデータ(Block Data)の先頭の4バイトを構成するブロック・シード(Block Seed)をセクタ2910において分離して、タイトル固有キー(Title Unique Key)との相互処理により、ブロックキー(Block Key)を生成する。

【0241】ブロック・キー(Block Key)の生成方法

は、先に説明した図14の構成を適用することができる。すなわち、32ビットのブロック・シード(Block Seed)と、64ビットのタイトル固有キー(Title Unique Key)とから、64ビットのブロックキー(Block Key)を生成する構成が適用できる。

【0242】なお、上記ではディスク固有キー(Disc Unique Key)、タイトル固有キー(Title Unique Key)、ブロックキー(Block Key)をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー(Disc Unique Key)とタイトル固有キー(Title Unique Key)の生成を実行することなく、ブロックごとにマスターキー(Master Key)とディスクID(Disc ID)とタイトルキー(Title Key)と、ブロックシード(Block Seed)と、デバイスID(再生機器制限をしない場合)もしくはデバイス固有キー(再生機器制限をする場合)を用いてブロックキー(Block Key)を生成してもよい。

【0243】ブロックキーが生成されると、ブロックキー(Block Key)を用いて暗号化されているブロックデータを復号2909し、セクタ2908を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにATSが付加されており、先に説明したTS処理手段300において、ATSに基づくストリーム処理が実行される。その後、データは、使用、たとえば、画像を表示したり、音楽を鳴らしたりすることが可能となる。

【0244】このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でATSを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。

【0245】次に図30に示すフローチャートに従って、復号処理および再生処理について、処理の流れを説明する。図30のS3001において、記録再生装置はディスクからディスクIDを、また自身のメモリからマスターキー、デバイスID、デバイス固有キーを読み出す。S3002で、ディスクIDとマスターキーを用いてディスク固有キーを生成する。

【0246】次にS3003で、ディスクから読み出すべきデータのタイトルキー、さらに、このデータを記録した記録再生器のデバイスIDと、データに対応して設定された再生機器制限フラグを読み出す。

【0247】次に、S3004で読み出すべきデータが再生可能か否かを判定する。判定の詳細を図31に示す。図31のステップS3101では、読み出した再生機器制限フラグの示す再生機器制限情報が、「再生機器制限あり」の設定であるか否かを判定する。ありの場合は、ステップS3102において、「記録媒体から読み出したデバイスIDと自己のデバイスIDが一致するか否か」を判定する。一致する場合は、再生可能と判定する。ステップS3101において、「再生機器制限あり」の設定でないと判定された場合も、再生可能と判定

する。読み出した再生機器制限フラグが示す再生機器制限情報が、「再生機器制限あり」かつ、「記録媒体から読み出したデバイスIDと自己のデバイスIDが一致しない」場合は、再生不可能と判定する。

【0248】次に、S3005で、タイトル固有キーの生成を行なう。タイトル固有キーの生成の詳細フローを図32に示す。暗号処理手段150は、ステップS3201において、再生機器制限をするの設定であるか、しないの設定であるかの判定を実行する。この判定は、ディスクから読み出した再生機器制限フラグに基づいて実行される。

【0249】S3201の判定がNo、すなわち、再生機器制限をしない設定である場合は、ステップS3202に進み、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、デバイスIDとから、タイトル固有キー (Title Unique Key) を生成する。

【0250】S3201の判定がYes、すなわち、再生機器制限をする場合は、ステップS3203に進みディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、自己の記録再生器の有するデバイス固有キーとから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【0251】次にS3006でディスクから暗号化されて格納されているブロックデータを読み出す。S3007で、ブロックデータの先頭の4バイトのブロックシード (Block Seed) と、S3005で生成したタイトル固有キーを用いてブロックキーを生成する。

【0252】次に、S3008で、ブロックキーを用いて暗号化されているブロックデータを復号し、S3009で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければS3006に戻り残りのデータを読み出す。

【0253】以上のように、再生機器制限をしない場合は、デバイスIDに基づいてブロックキーを生成し、再生機器制限をする場合は、デバイス固有キーに基づいてブロックキーを生成するという2つの設定が可能であり、いずれかの設定に基づいてコンテンツをブロック単位で暗号化して記録媒体に格納することができる。記録媒体に格納されたデータを再生する場合、デバイス固有キーに基づいて暗号化されたデータに関しては、そのデータを記録した機器でのみ再生可能とする構成となり、再生機器制限をしない場合は、ディスクに記録したデバイスIDを用いて他の機器がブロックキーを生成することが可能となるので他の機器における復号処理、再生処理を実行を可能とすることができる。

【0254】〔記録処理におけるコピー制御〕さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【0255】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの (コピー可能) かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【0256】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図1または図2の記録再生装置の処理について、図33および図34のフローチャートを参照して説明する。

【0257】まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図33

(A) のフローチャートにしたがった記録処理が行われる。図33 (A) の処理について説明する。図1の記録再生器100を例として説明する。デジタル信号のコンテンツ (デジタルコンテンツ) が、例えば、IEEE1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS3301において、入出力I/F120は、そのデジタルコンテンツを受信し、ステップS3302に進む。

【0258】ステップS3302では、入出力I/F120は、受信したデジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力I/F120が受信したコンテンツが暗号化されていない場合 (例えば、上述のDTCPを使用せずに、平文のコンテンツが、入出力I/F120に供給された場合) には、そのコンテンツは、コピー可能であると判定される。

【0259】また、記録再生装置100がDTCPに準拠している装置であるとし、DTCPに従って処理を実行するものとする。DTCPでは、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator) が規定されている。EMIが00B (Bは、その前の値が2進数であることを表す) である場合は、コンテンツがコピーフリーのもの (Copy-free) であることを表し、EMIが01Bである場合には、コンテンツが、それ以上のコピーをすることができないもの (No-more-copies) であることを表す。さらに、EMIが10Bである場合は、コンテンツが、1度だけコピーして良いもの (Copy-one-generation) であることを表し、EMIが11Bである場合には、コンテンツが、コピーが禁止されているもの (Copy-never) であることを表す。

【0260】記録再生装置100の入出力I/F120に供給される信号にEMIが含まれ、そのEMIが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、EMIが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【0261】ステップS3302において、コンテンツがコピー可能でないと判定された場合、ステップS3303～S3305をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体195に記録されない。

【0262】また、ステップS3302において、コンテンツがコピー可能であると判定された場合、ステップS3303に進み、以下、ステップS3303～S3305において、図3(A)のステップS302、S303、S304における処理と同様の処理が行われる。すなわち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0263】なお、EMIは、入出力I/F120に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、EMI、あるいは、EMIと同様にコピー制御状態を表す情報（例えば、DTCFにおけるembedded CCIなど）も記録される。

【0264】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【0265】本発明の記録再生装置では、このEMIやembedded CCIなどのコピー制御情報を、TSパケットに付加する形で記録する。即ち、図10の例2や例3のように、ATSを24ビットないし30ビット分と、コピー制御情報を加えた32ビットを図5に示すように各TSパケットに付加する。

【0266】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図33(B)のフローチャートにしたがった記録処理が行われる。図33(B)の処理について説明する。アナログ信号のコンテンツ（アナログコンテンツ）が、入出力I/F140に供給されると、入出力I/F140は、ステップS3311において、そのアナログコンテンツを受信し、ステップS3312に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【0267】ここで、ステップS3312の判定処理は、例えば、入出力I/F140で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力I/F140で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【0268】また、例えば、CGMS-A信号は、デジタル信号のコピー制御に用いられるCGMS信号を、

アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

【0269】従って、CGMS-A信号が、入出力I/F140で受信した信号に含まれ、かつ、そのCGMS-A信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【0270】さらに、例えば、マクロビジョン信号も、CGMS-A信号も、入出力I/F4で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【0271】ステップS3312において、アナログコンテンツがコピー可能でないと判定された場合、ステップS3313乃至S3317をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体195に記録されない。

【0272】また、ステップS3312において、アナログコンテンツがコピー可能であると判定された場合、ステップS3313に進み、以下、ステップS3313乃至S3317において、図3(B)のステップS322乃至S326における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、MPEG符号化、TS処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【0273】なお、入出力I/F140で受信したアナログ信号に、CGMS-A信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのCGMS-A信号も、記録媒体に記録される。即ち、図10で示したCCIもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0274】[再生処理におけるコピー制御] 次に、記録媒体に記録されたコンテンツを再生して、デジタルコンテンツとして外部に出力する場合においては、図34(A)のフローチャートにしたがった再生処理が行われる。図34(A)の処理について説明する。まず最初に、ステップS3401、S3402、S3403において、図4(A)のステップS401、S402、S403における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理

手段150において復号処理がなされ、TS処理がなされる。各処理が実行されたデジタルコンテンツは、バス110を介して、入出力I/F120に供給される。

【0275】入出力I/F120は、ステップS3404において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI、あるいは、EMIと同様にコピー制御状態を表す情報（コピー制御情報）が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0276】また、例えば、入出力I/F120に供給されるデジタルコンテンツにEMIが含まれる場合、従って、コンテンツの記録時に、DTC Pの規格にしたがって、EMIが記録された場合には、そのEMI（記録されたEMI（Recorded EMI））が、Copy-freelyであるときには、デジタルコンテンツは、後でコピー可能なものであると判定される。また、EMIが、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないとは判定される。

【0277】なお、一般的には、記録されたEMIが、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのEMIは記録時にNo-more-copiesに変換され、また、Copy-neverのEMIを持つデジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0278】ステップS3404において、コンテンツが、後でコピー可能なものであると判定された場合、ステップS3405に進み、入出力I/F120は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

【0279】また、ステップS3404において、コンテンツが、後でコピー可能なものでないとは判定された場合、ステップS3406に進み、入出力I/F120は、例えば、DTC Pの規格等にしたがって、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0280】即ち、例えば、上述のように、記録されたEMIが、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMIがCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0281】このため、入出力I/F120は、DTC

Pの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、DTC Pの規格に準拠した装置である場合）には、デジタルコンテンツを暗号化して、外部に出力する。

【0282】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図34（B）のフローチャートにしたがった再生処理が行われる。図34（B）の処理について説明する。ステップS3411乃至S3415において、図4（B）のステップS421乃至S425における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、TS処理、MPEGデコード、D/A変換が実行される。これにより得られるアナログコンテンツは、入出力I/F140で受信される。

【0283】入出力I/F140は、ステップS3416において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツと共にコピー制御情報が記録されていなかった場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0284】また、コンテンツの記録時に、たとえばDTC Pの規格にしたがって、EMIまたはコピー制御情報が記録された場合には、そのEMIまたはコピー制御情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【0285】また、EMIまたはコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMIまたはコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないとは判定される。

【0286】さらに、例えば、入出力I/F140に供給されるアナログコンテンツにCGMS-A信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにCGMS-A信号が記録された場合には、そのCGMS-A信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、CGMS-A信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないとは判定される。

【0287】ステップS3416において、アナログコンテンツが、後でコピー可能であると判定された場合、ステップS3417に進み、入出力I/F140は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【0288】また、ステップS3416において、アナログコンテンツが、後でコピー可能でないと判定された

場合、ステップS 3 4 1 8に進み、入出力I / F 1 4 0は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0289】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0290】このため、入出力I / F 1 4 0は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すGCMS-A信号を付加して、外部に出力する。また、例えば、記録されたGCMS-A信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力I / F 4は、GCMS-A信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【0291】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【0292】【データ処理手段の構成】なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段150は暗号化／復号LSIとして構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にTS処理手段300も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図35は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【0293】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク3505やROM3503に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magnetooptical) ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体3510に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体3510は、いわゆるパッケージソフトウェアとして提供することができる。

【0294】なお、プログラムは、上述したようなリムーバブル記録媒体3510からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部3508で受信し、内蔵するハードディスク3505にインストールすることができる。

【0295】コンピュータは、CPU (Central Processing Unit) 3502を内蔵している。CPU 3502には、バス3501を介して、入出力インタフェース3511が接続されており、CPU 3502は、入出力インタフェース3510を介して、ユーザによって、キーボードやマウス等で構成される入力部3507が操作されることにより指令が入力されると、それにしたがって、ROM (Read Only Memory) 3503に格納されているプログラムを実行する。

【0296】あるいは、CPU 3502は、ハードディスク3505に格納されているプログラム、衛星若しくはネットワークから転送され、通信部3508で受信されてハードディスク3505にインストールされたプログラム、またはドライブ3509に装着されたリムーバブル記録媒体3510から読み出されてハードディスク3505にインストールされたプログラムを、RAM (Random Access Memory) 3504にロードして実行する。

【0297】これにより、CPU 3502は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU 3502は、その処理結果を、必要に応じて、例えば、入出力インタフェース3511を介して、LCD (Liquid Crystal Display) やスピーカ等で構成される出力部3506から出力、あるいは、通信部3508から送信、さらには、ハードディスク3505に記録させる。

【0298】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0299】また、プログラムは、1つのコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0300】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図1およ

び図2に示すCPU170が実行する1つのソフトウェアモジュールとして実現することも可能である。同様に、TS処理手段300の処理もCPU170が実行する1つのソフトウェアモジュールとして実現することが可能である。

【0301】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0302】

【発明の効果】本発明の情報記録再生装置および方法によれば、各パケットの着信時刻に応じたランダム性のあるデータとして構成されるATSを用いてブロック・データを暗号化するブロックキーを生成する構成としたので、ブロック毎に異なる固有キーを生成することが可能となり、ブロックごとに暗号鍵を変更でき、暗号解析に対する強度を高めることができる。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【図面の簡単な説明】

【図1】本発明の情報記録再生装置の構成例（その1）を示すブロック図である。

【図2】本発明の情報記録再生装置の構成例（その2）を示すブロック図である。

【図3】本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図4】本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図5】本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

【図6】本発明の情報記録再生装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図7】本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

【図8】本発明の情報記録再生装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図9】本発明の情報記録再生装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図10】本発明の情報記録再生装置において処理され

るブロックデータの付加情報としてのブロック・データの構成例を示す図である。

【図11】本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その1）である。

【図12】本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その2）である。

【図13】本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ記録処理時の暗号化処理を説明するフローチャートである。

【図14】本発明の情報記録再生装置におけるブロック・キーの生成方法を説明する図である。

【図15】本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

【図16】本発明の情報記録再生装置において、データ互換性の要請されるシステムにおけるデータ再生処理時の復号処理を説明するフローチャートである。

【図17】本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図である。

【図18】本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ記録処理時の暗号化処理を説明するフローチャートである。

【図19】本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデバイス固有キー生成処理例（その1）を説明するブロック図である。

【図20】本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデバイス固有キー生成処理例（その2）を説明するブロック図である。

【図21】本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

【図22】本発明の情報記録再生装置において、データ互換性の要請されないシステムにおけるデータ再生処理時の復号処理を説明するフローチャートである。

【図23】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その1）である。

【図24】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理時の暗号化処理を説明するブロック図（その2）である。

【図25】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録処理を説明するフローチャートである。

【図26】本発明の情報記録再生装置におけるディスク固有キーの生成例を説明する図である。

【図27】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるタイトル固有キーの生成

処理フローを示す図である。

【図28】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ記録時のタイトル固有キーの生成処理例を示す図である。

【図29】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理時の復号処理を説明するブロック図である。

【図30】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理を説明するフローチャートである。

【図31】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

【図32】本発明の情報記録再生装置において、再生機器制限可能なシステムにおけるデータ最盛時のタイトル固有キーの生成処理フローを示す図である。

【図33】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図34】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

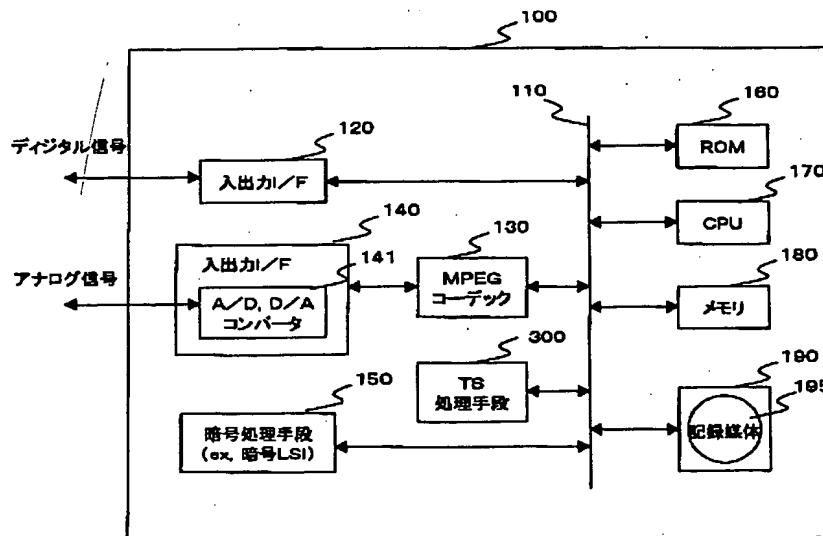
【図35】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

【符号の説明】

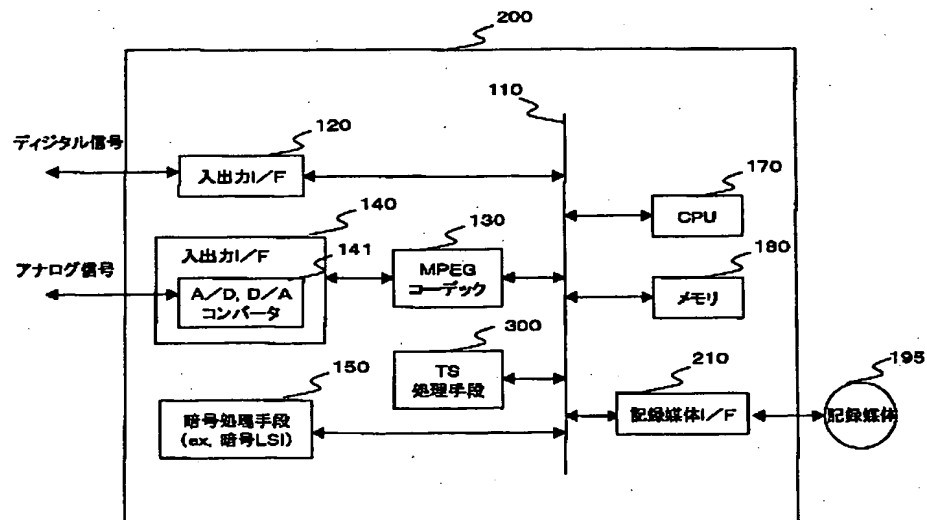
100, 200 記録再生装置
110 バス
120 入出力 I/F
130 MPEGコーデック
140 入出力 I/F
141 A/D, D/Aコンバータ
150 暗号処理手段
160 ROM
170 CPU
180 メモリ
190 ドライブ

195 記録媒体
210 記録媒体 I/F
300 TS処理手段
600, 607 端子
602 ビットストリームパーサー
603 PLL
604 タイムスタンプ発生回路
605 ブロックシード付加回路
606 スムージングバッファ
800, 806 端子
801 ブロックシード分離回路
802 出力制御回路
803 比較器
804 タイミング発生回路
805 27MHzクロック
901, 904, 913 端子
902 MPEGビデオエンコーダ
903 ビデオストリームバッファ
905 MPEGオーディオエンコーダ
906 オーディオストリームバッファ
908 多重化スケジューラ
909 トランスポートバケット符号化器
910 到着タイムスタンプ計算手段
911 ブロックシード付加回路
912 スムージングバッファ
976 スイッチ
3501 バス
3502 CPU
3503 ROM
3504 RAM
3505 ハードディスク
3506 出力部
3507 入力部
3508 通信部
3509 ドライブ
3510 リムーバブル記録媒体
3511 入出力インタフェース

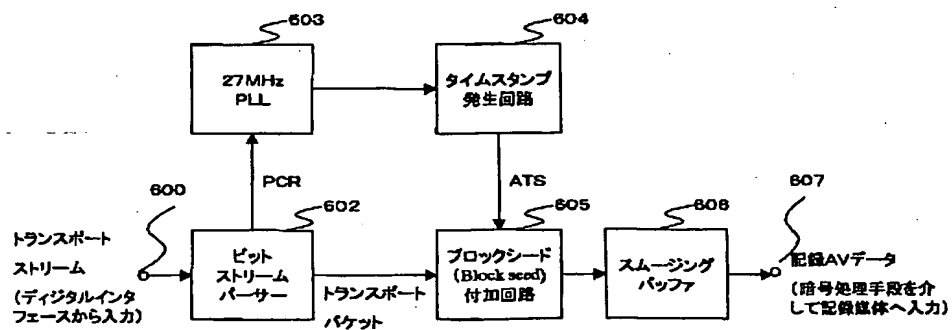
【図 1】



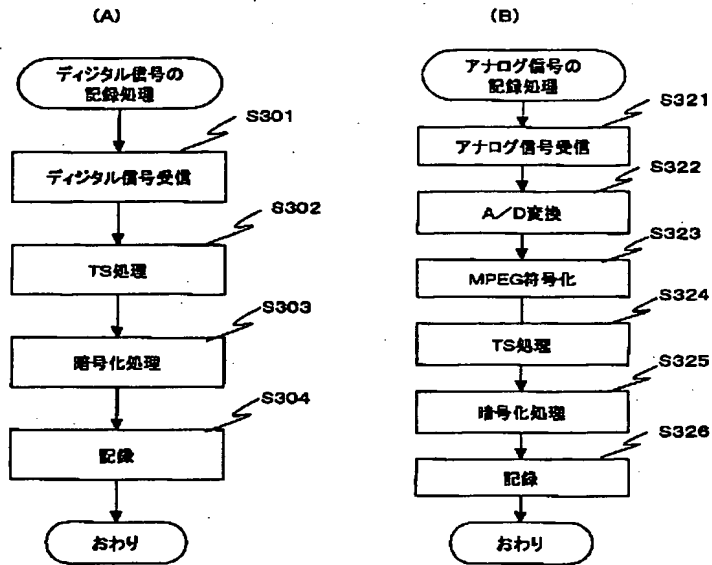
【図 2】



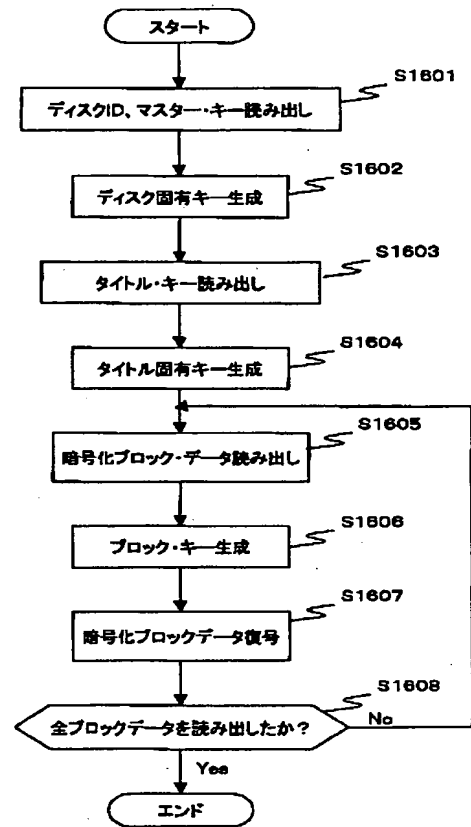
【図 6】



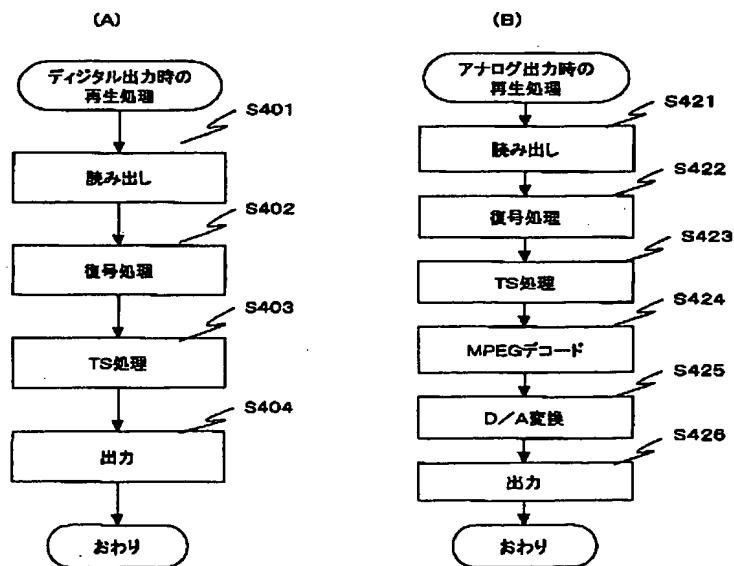
【図3】



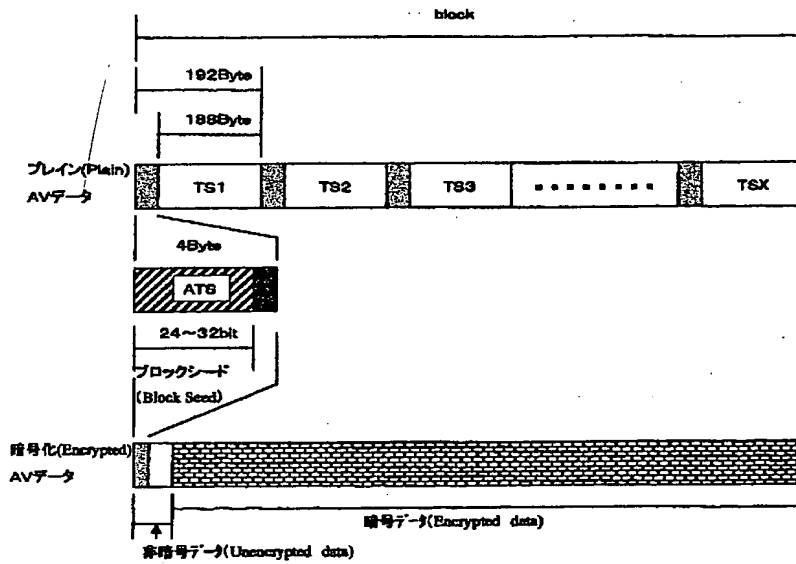
【図16】



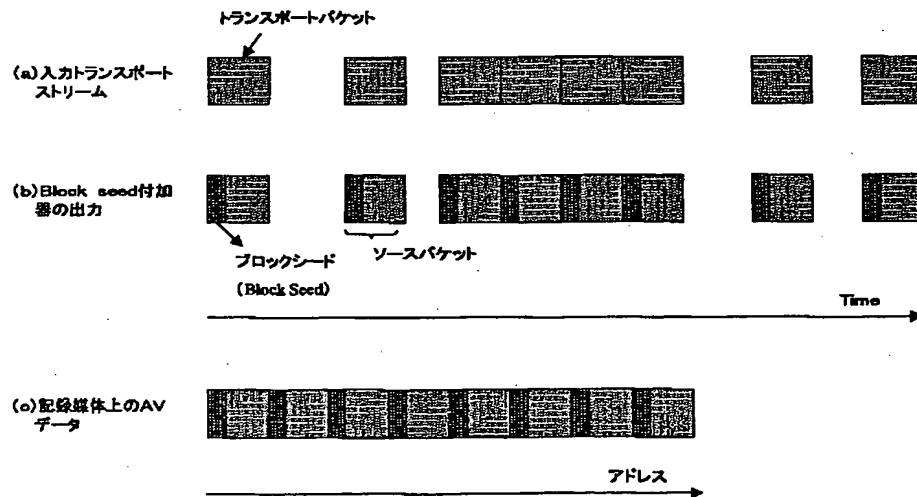
【図4】



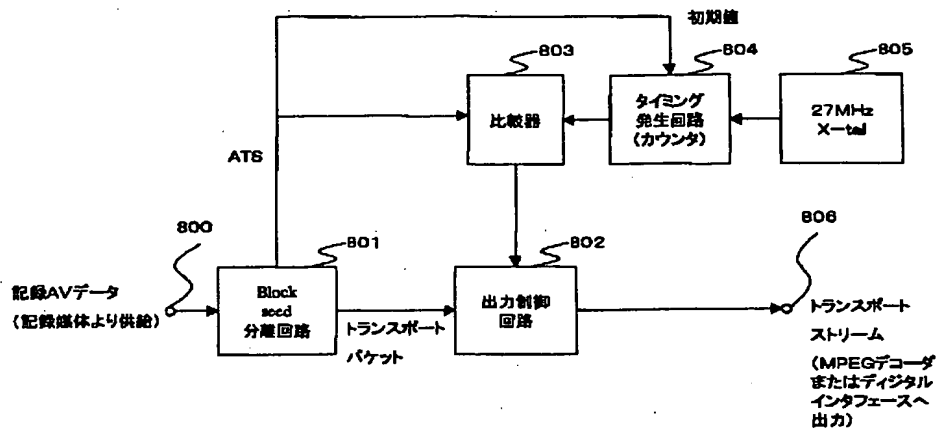
【図5】



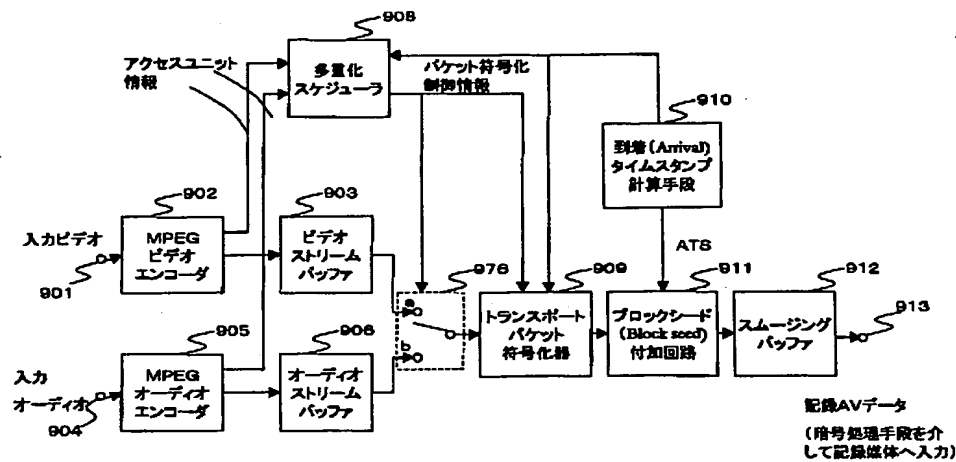
【図7】



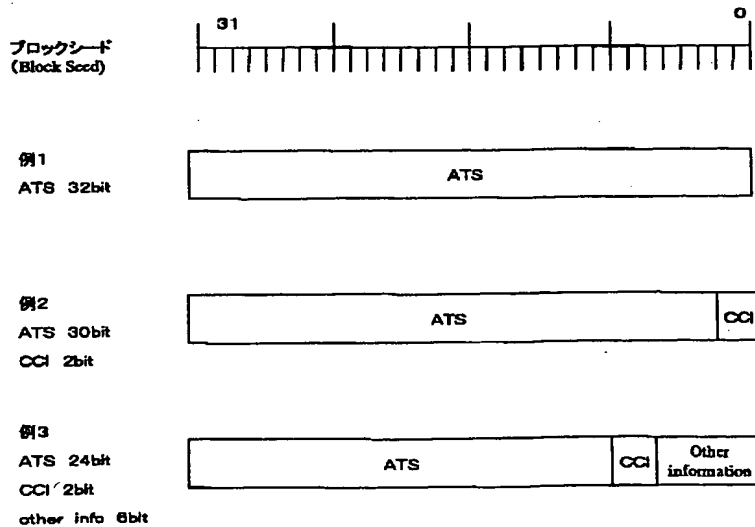
【図8】



【図9】



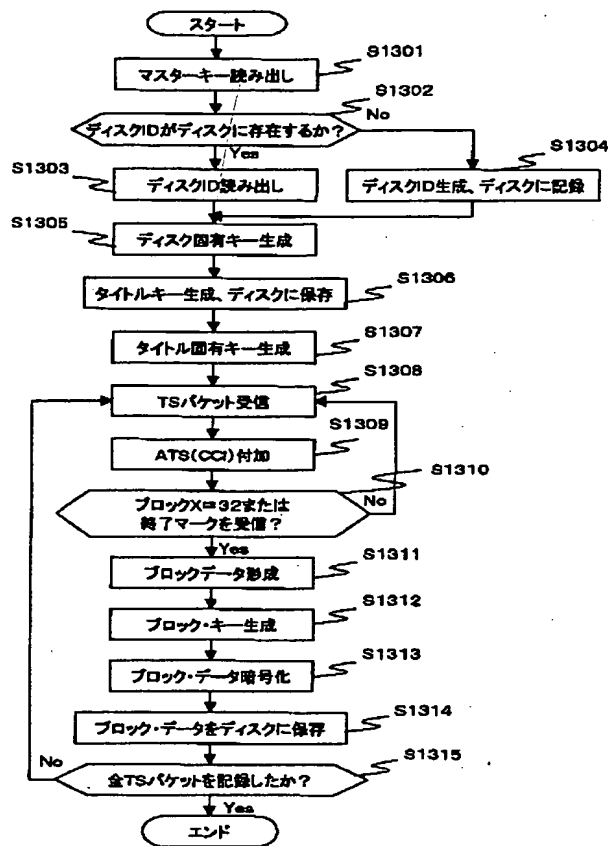
【図10】



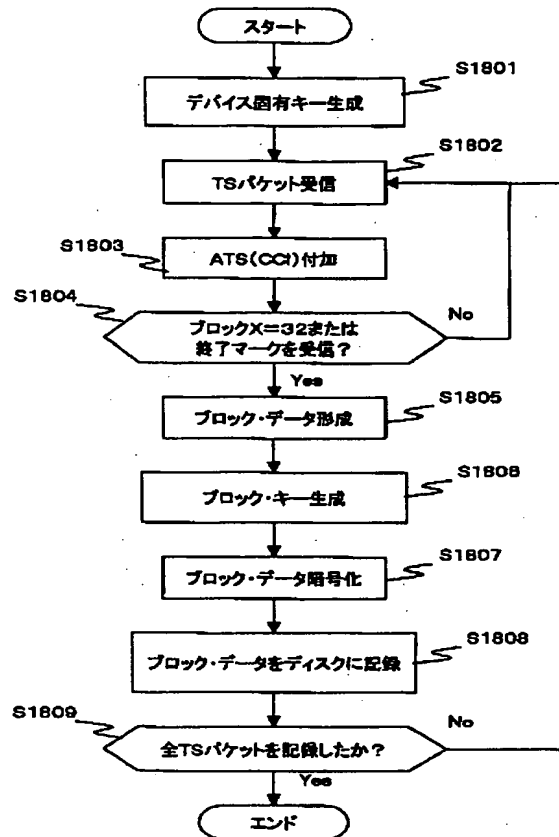
The diagram illustrates the internal components and data flow of the encryption system. It includes blocks for generating unique keys for disks and titles, generating block keys, performing encryption, and selecting specific bytes of data. The process starts with input data being encrypted using a disk key and a title key to produce encrypted content. This content is then processed by a block key generation unit and a selection unit to produce the final output.

互換性が必要なシステム(記録時)

【図13】



【図18】



【図14】

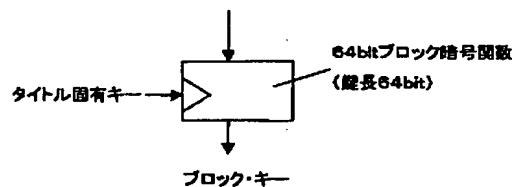
例1

ブロックキー生成例

入力
 ブロック・シード(32bit)
 タイトル固有キー(64bit)

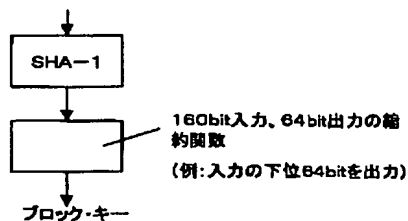
出力
 ブロック・キー(64bit)

ブロック・シード||コンスタント(32bit)

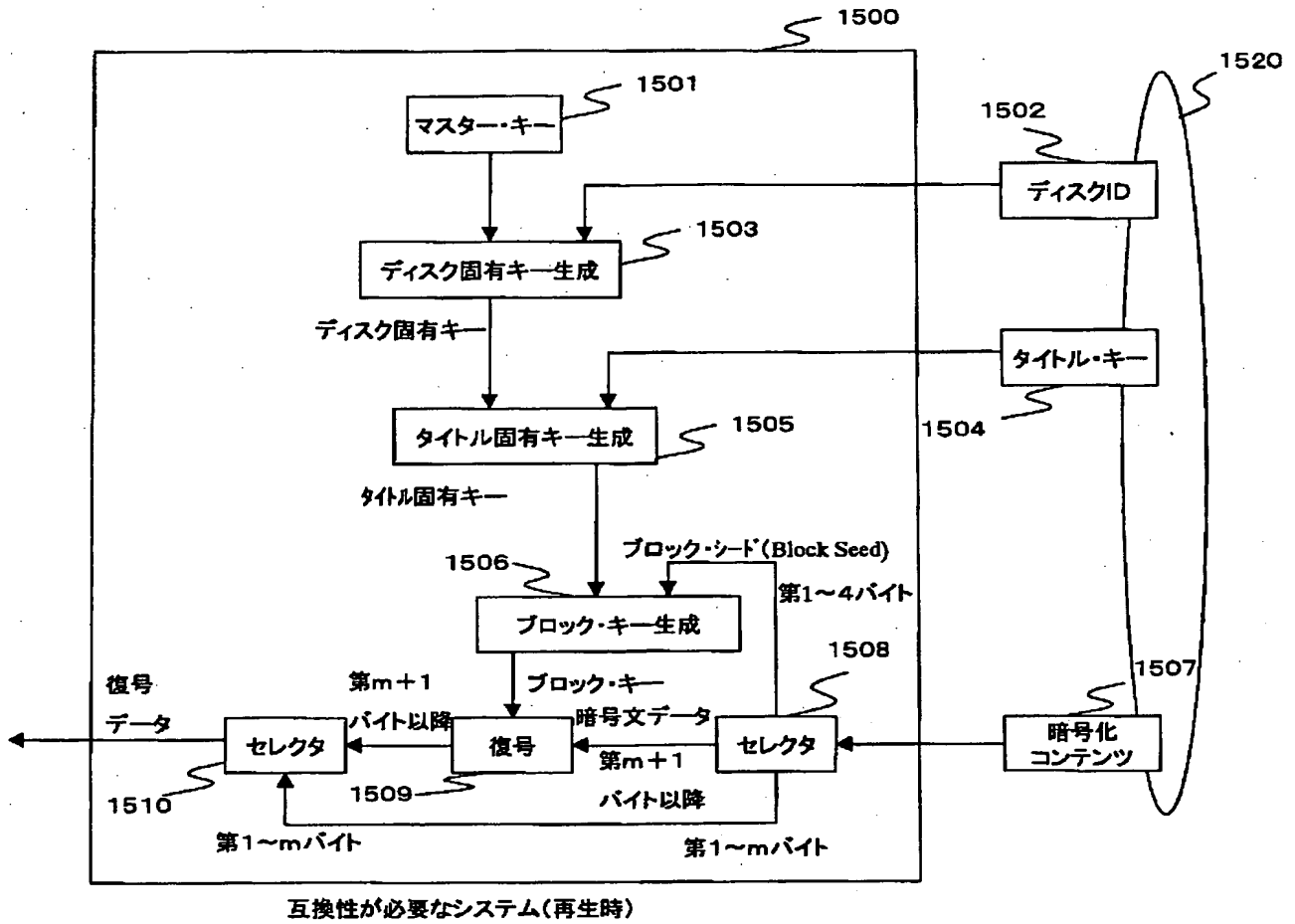


例2

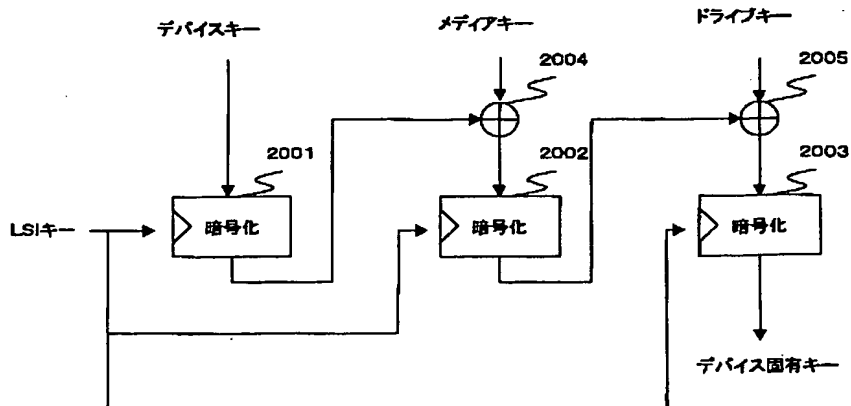
タイトル固有キー||ブロック・シード



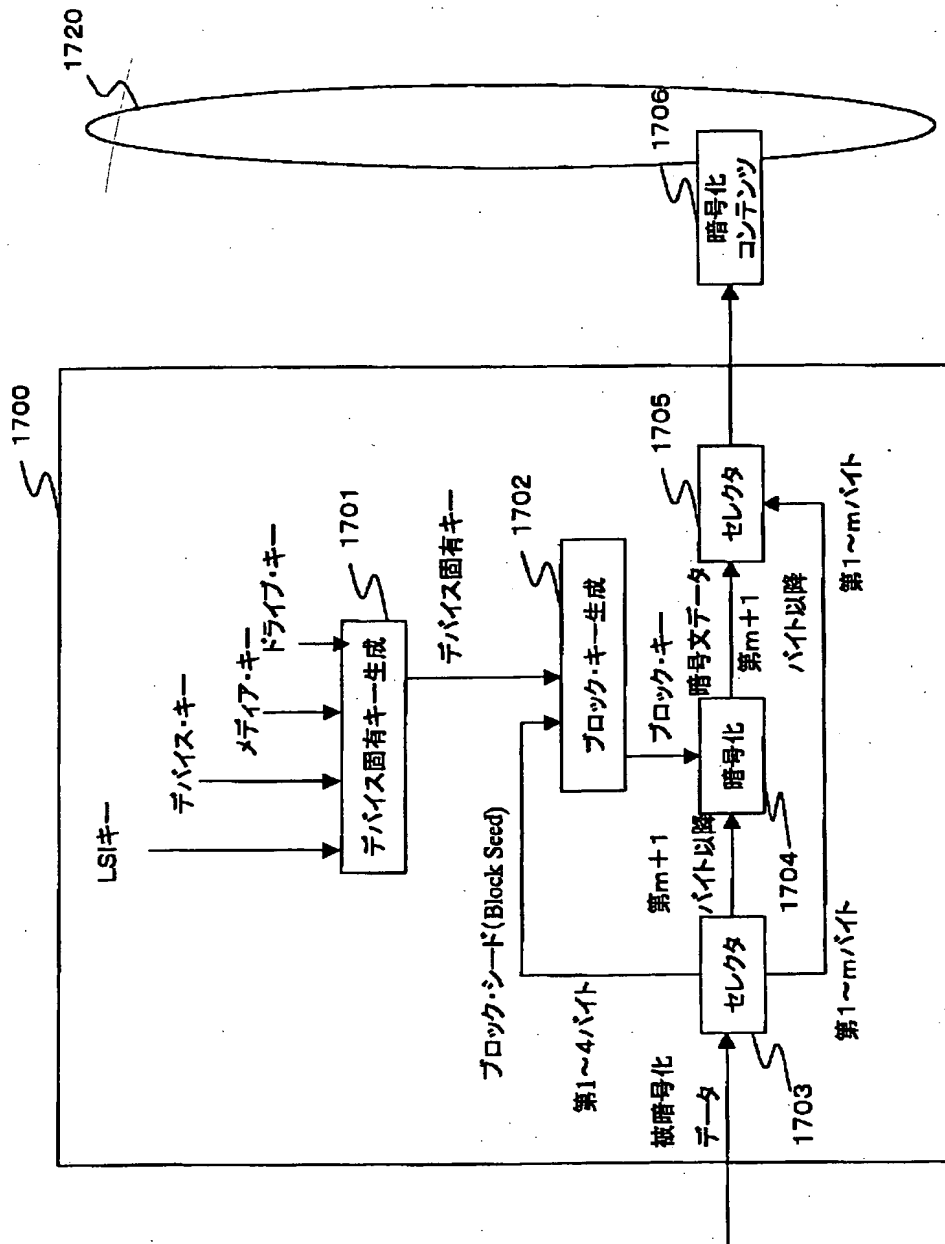
【図15】



【図20】

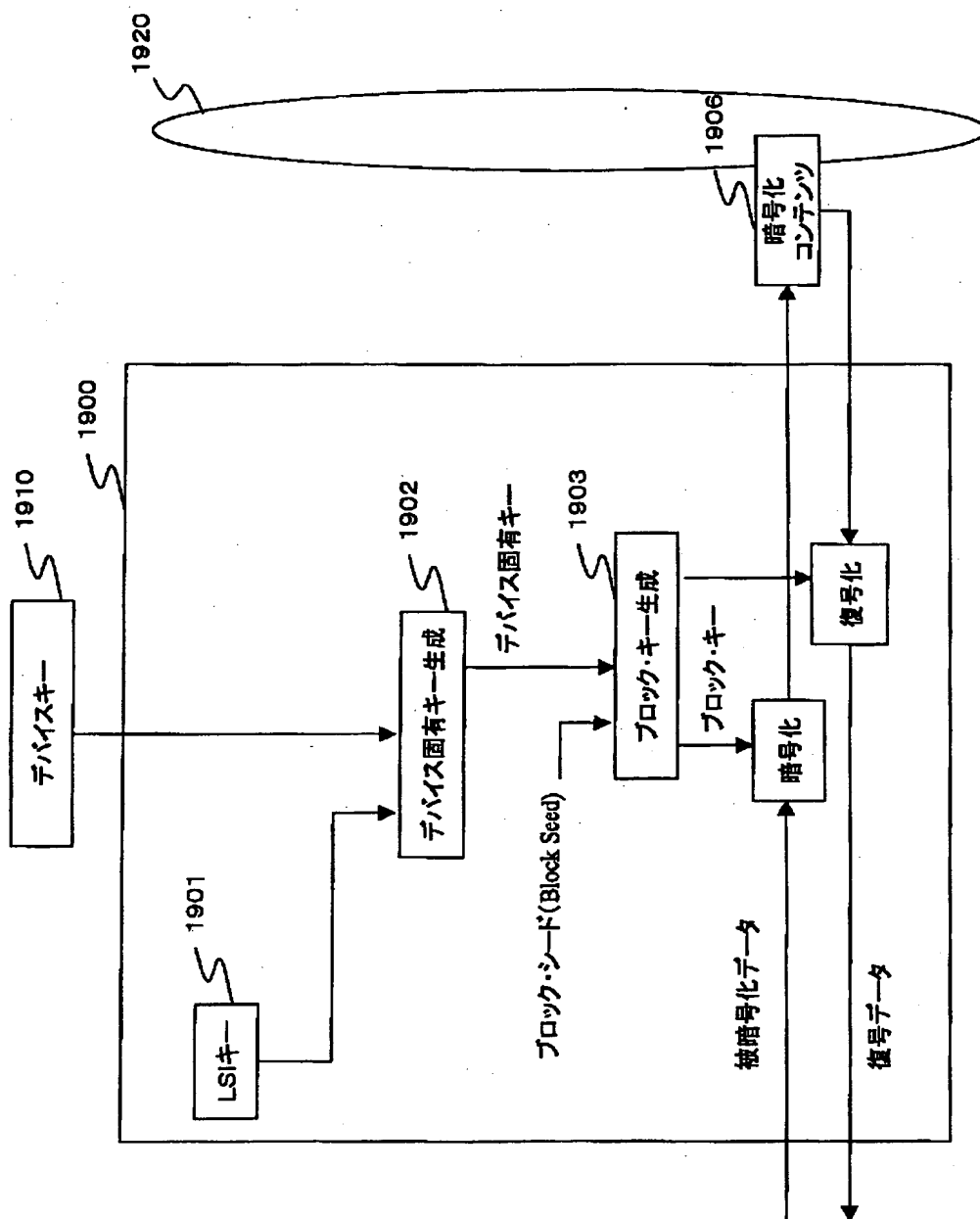


【図17】

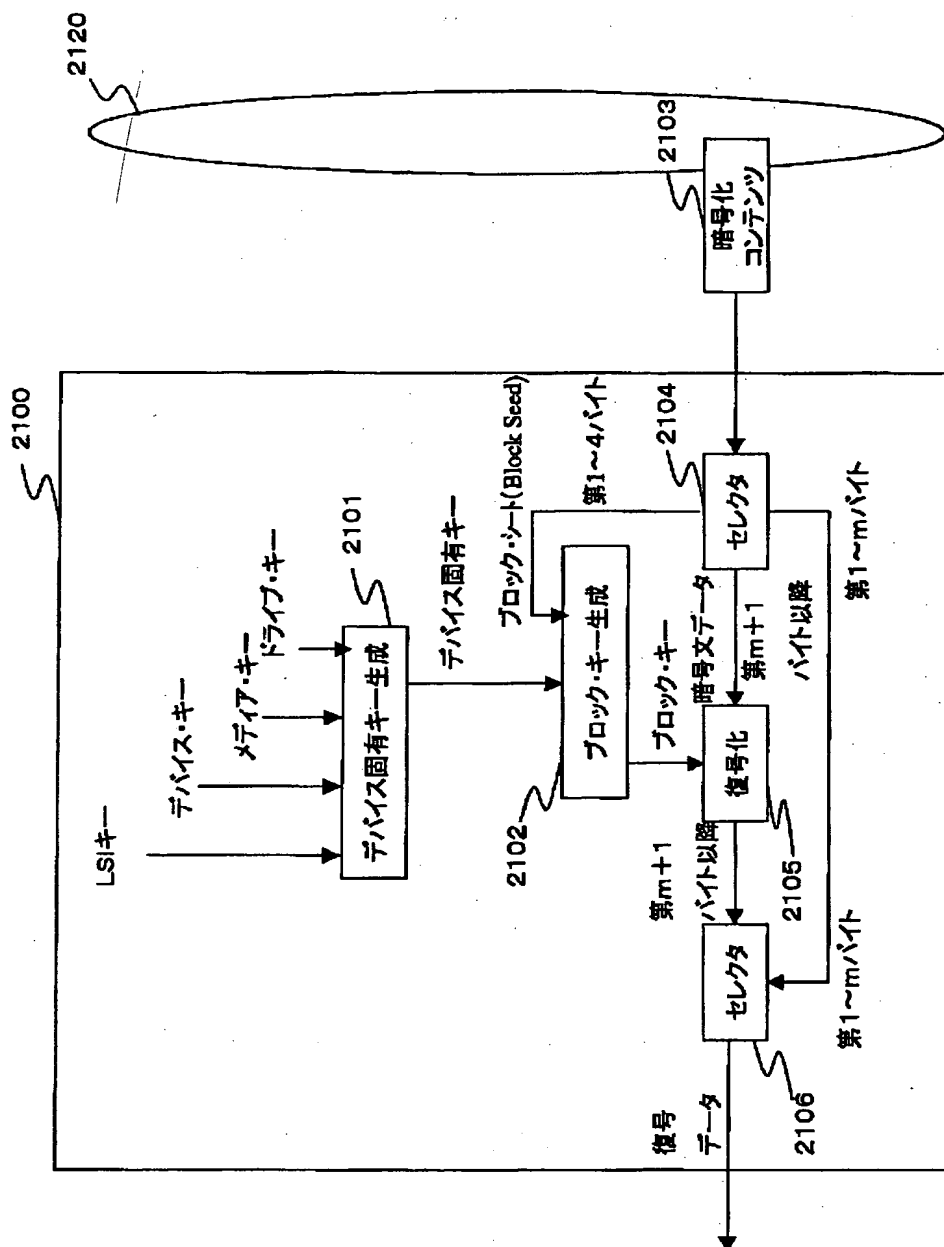


互換性が必要でないシステム(記録時)

【図19】

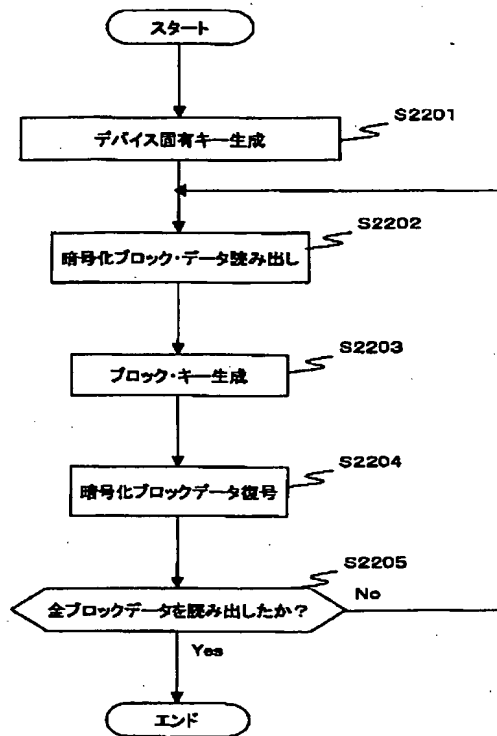


【図21】

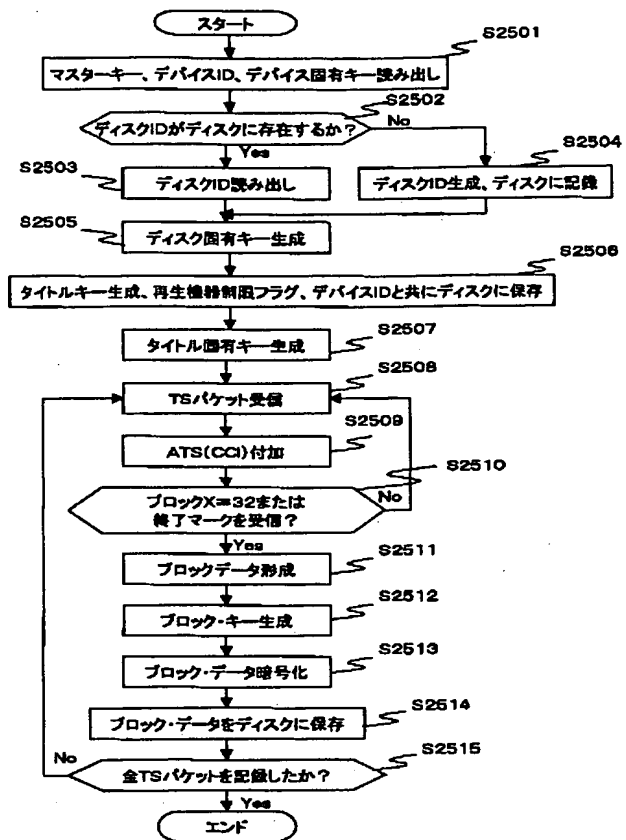


互換性が必要でないシステム(再生時)

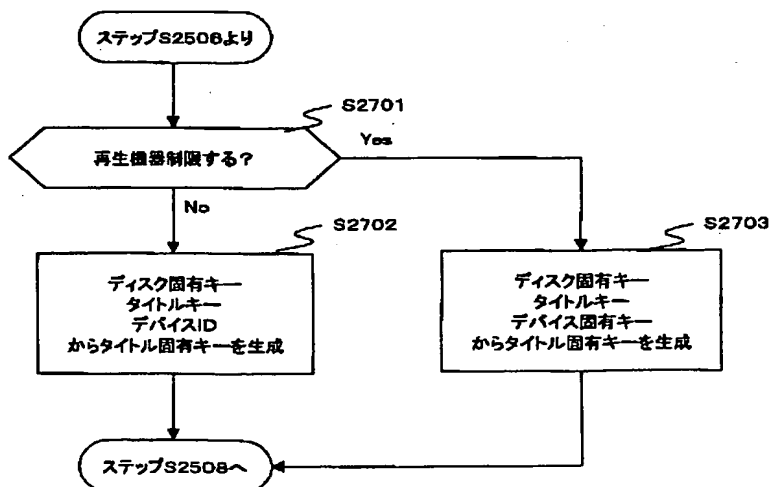
【図22】



【図25】



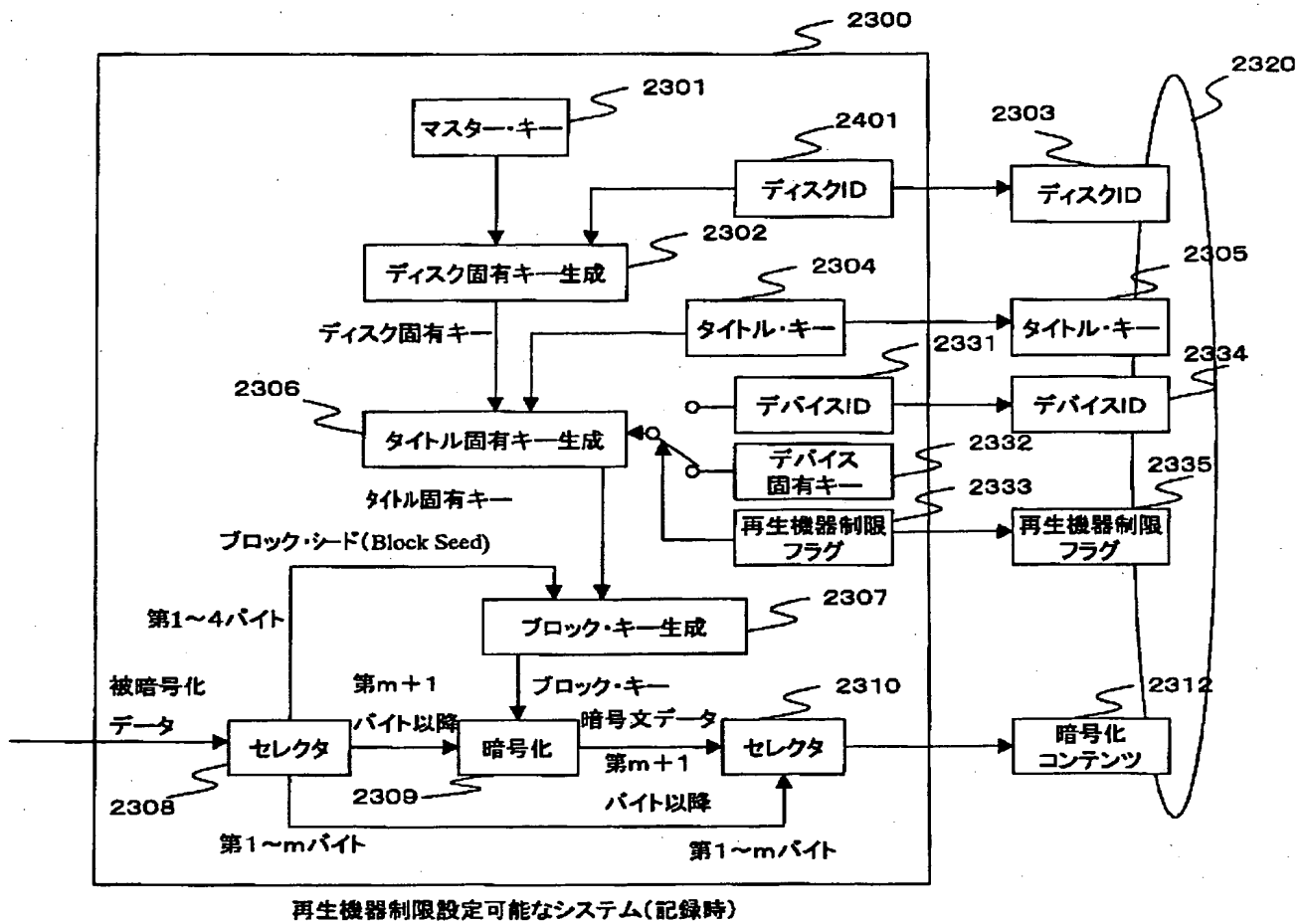
【図27】



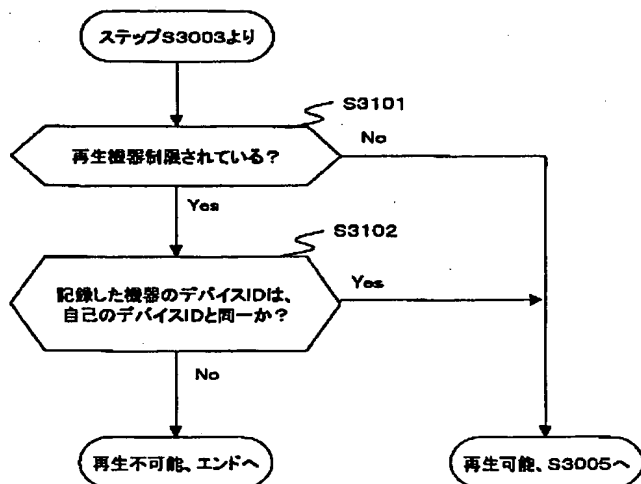
[illegible]

再生機器制限設定可能なシステム(記録時)

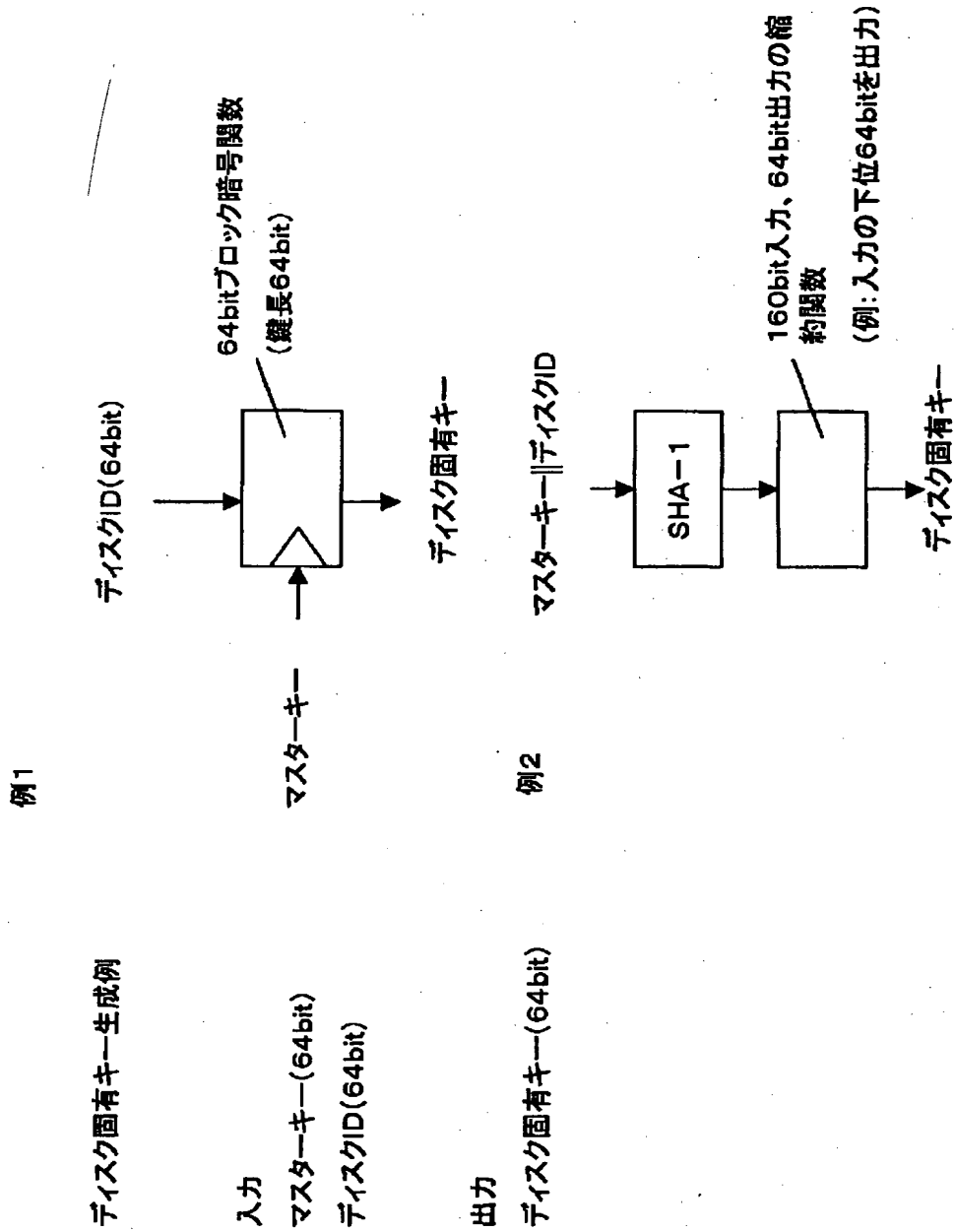
【図24】



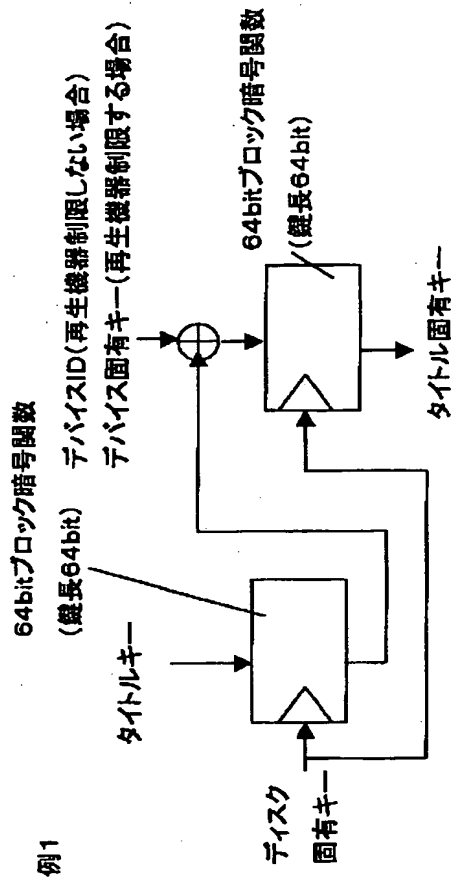
【図31】



【図26】



【図28】



タイトル固有キー生成例

入力

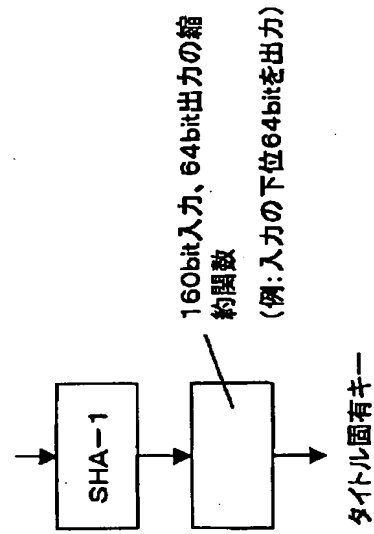
ディスク固有キー(64bit)
タイトルキー(64bit)デバイスID(64bit)または
デバイス固有キー(64bit)

例2

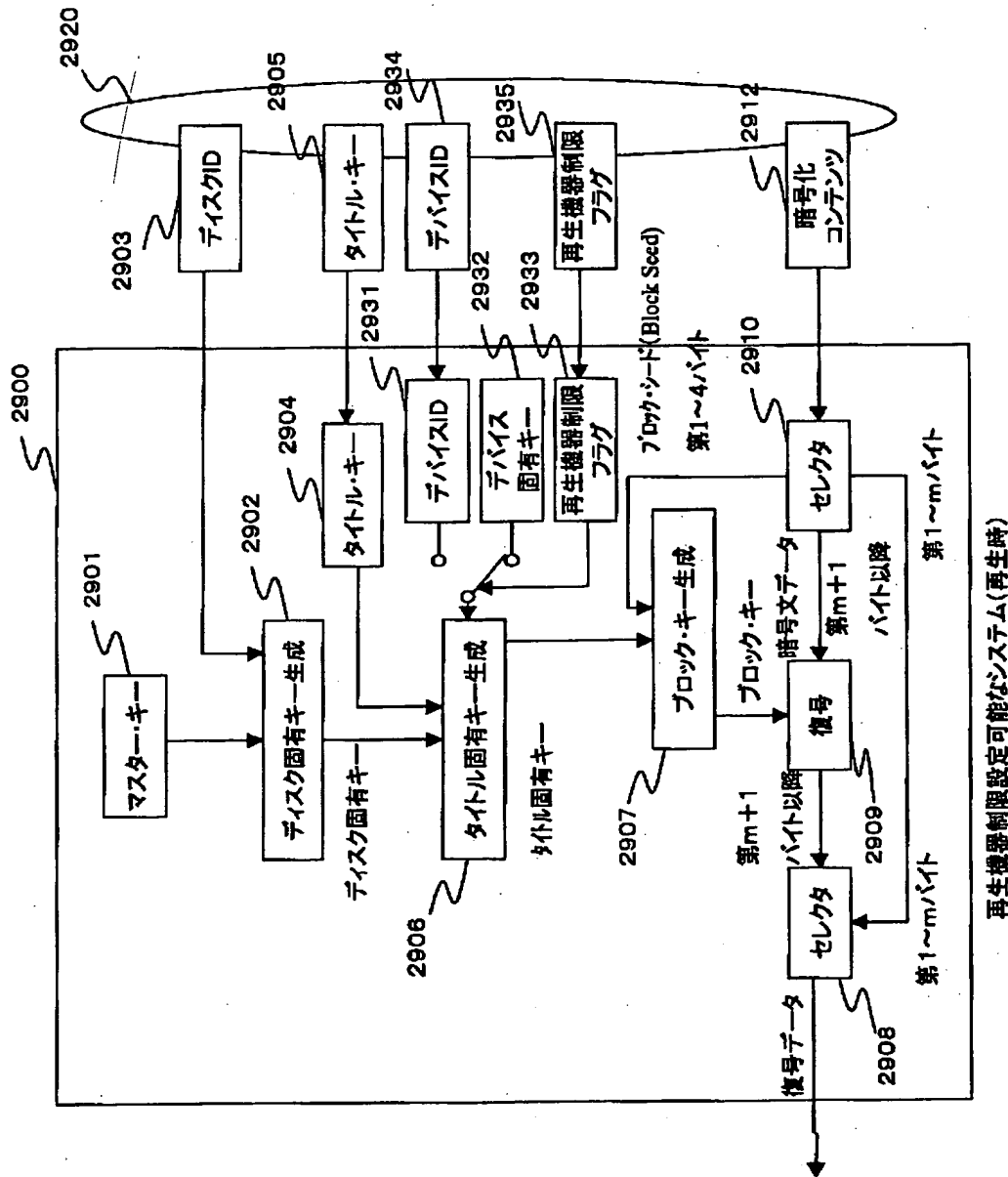
ディスク固有キー||タイトルキー||デバイスID(再生機器制限しない場合)

タイトル固有キー(64bit)

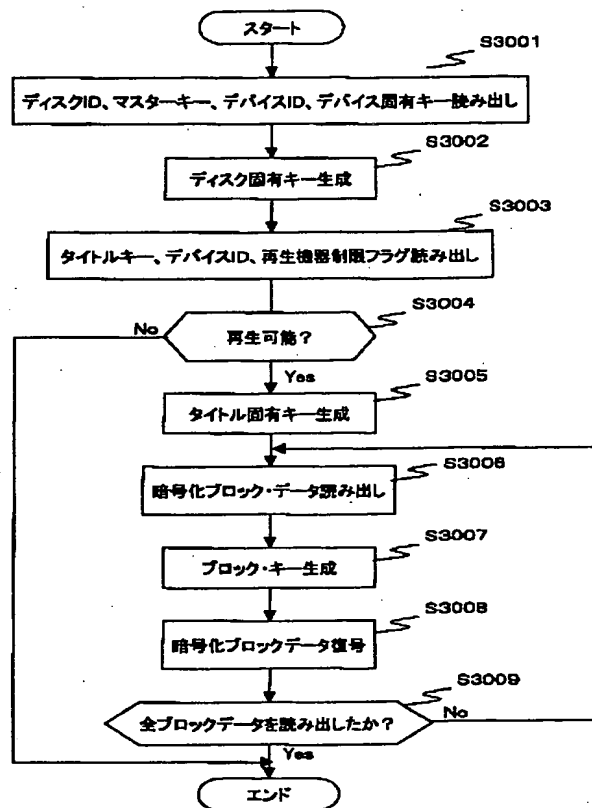
ディスク固有キー||タイトルキー||デバイス固有キー(再生機器制限する場合)



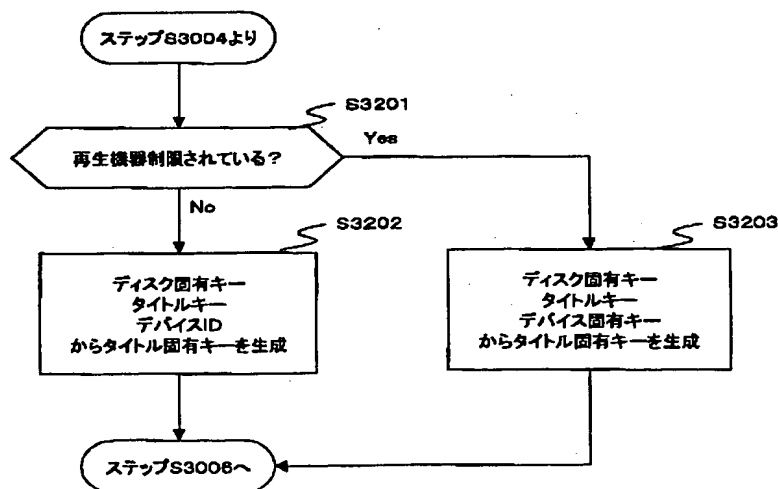
【図29】



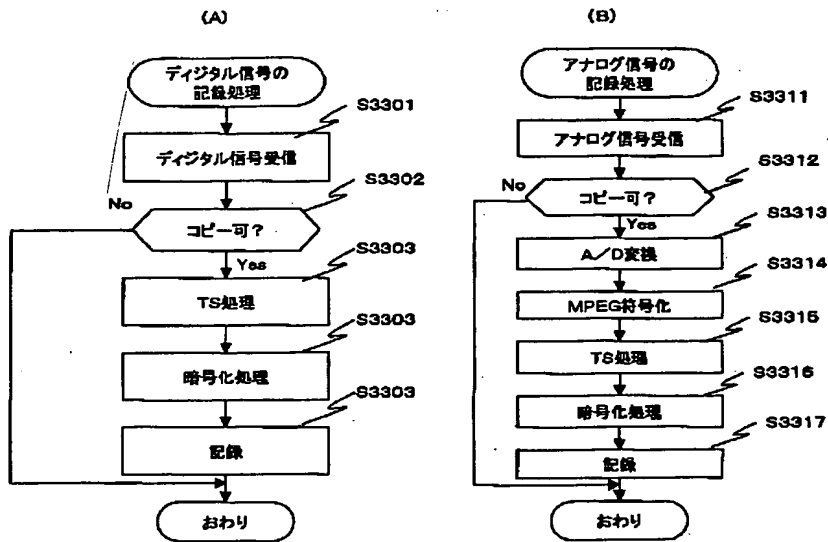
【図30】



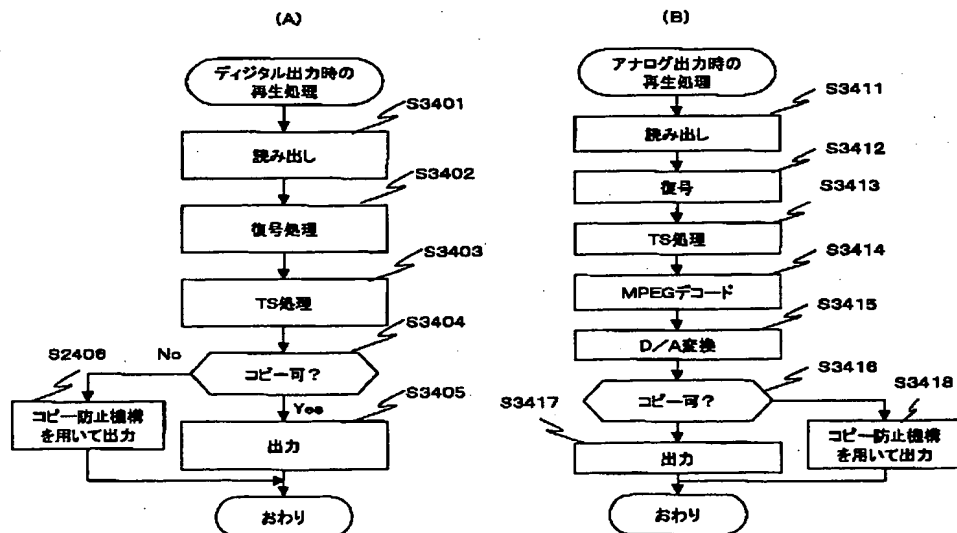
【図32】



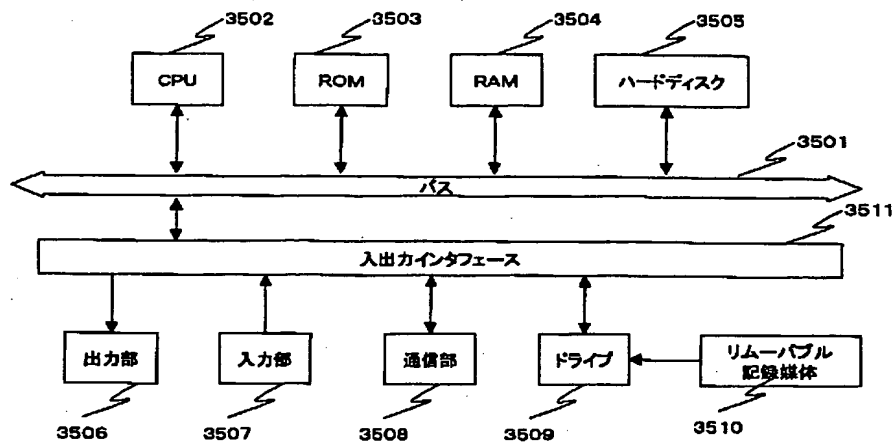
【図33】



【図34】



【図35】



フロントページの続き

(72)発明者 加藤 元樹
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

Fターム(参考) 5C053 FA13 FA23 GA20 GB01 GB05
GB37 JA21 LA15
5D044 AB05 AB07 BC01 BC06 CC01
CC06 DE23 DE39 DE49 DE53
EF05 FG18 GK17 HL02 HL08
5J104 AA01 AA13 AA16 AA34 AA35
EA07 NA02 PA14